PRISM

VOL. 12, NO. 1 | FALL 2026

PRISM
VOL. 12, NO. 1, FALL 2026

EDITOR-IN-CHIEF
John A. Pennell, Ph.D.

ASSOCIATE EDITORS
COL Kevin D. Stringer, USA (Ret.), Ph.D.
Joshua A. Hastey, Ph.D.
Sandor Fabian, Ph.D.

EDITOR-IN-CHIEF EMERITUS
Michael Miklaucic

MANAGING EDITOR
SGM Kanessa R. Trent, USA (Ret.), MEd.

EDITORIAL ASSISTANT
V. Jocelynne Lake

DESIGN
Jamie Harvey, U.S. Government Publishing Office

EDITORIAL ADVISORS
AMB (ret.) Art Brown
COL (ret.) Prof. David A. Brown
Candice Bryant
Melanie Casey
Dr. William T. Eliason
Dr. Amos Fox
Dr. Whitney Grespin
CAPT (ret.) William Hamblet
AMB (ret.) Philip S. Kosnett
Dr. Ajit Maan
Dr. Asta Maskaliunaite
Dr. C. Anthony Pfaff
Beth E. Sanner
Dr. George Spencer Terry
Dr. Michael G. Vickers
GEN (ret.) Joseph L. Votel
Dr. Vivian Walker
Prof. Jeffrey Zinsmeister, JD

ISSN 2157- 0663

ABOUT

PRISM: The Journal of Emerging Threats | Complex Statecraft is the U.S. Department of War (DOW) Irregular Warfare Center's (IWC) flagship journal of national and international security affairs. *PRISM*, which is published semiannually, aims to "provide unique insight for current and future national security leaders on emerging security challenges beyond the strictly military domain of the joint force, including transnational, multi-domain threats, gray zone conflict, the technological innovation challenge, and geo-economic competition among the great powers." For more information, visit our website at https://irregularwarfarecenter.org/prism/.

SUBMISSIONS

PRISM: The Journal of Emerging Threats | Complex Statecraft welcomes unsolicited manuscripts from policymakers, practitioners, and scholars, particularly those that present fresh thought, enduring insight, or best practices related to the emerging national security environment. We seek to publish provocative, insightful, and well-reasoned submissions. We welcome contributions not only from established authorities in the field but also emerging voices, including early career practitioners, policymakers, and scholars. *PRISM* accepts three types of submissions:

- Research articles
- Standard book reviews
- Extended book reviews

For additional information on submission requirements and the review process, visit our website at https://irregularwarfarecenter.org/prism/ or contact us at PRISM@irregularwarfarecenter.org.

DISCLAIMER

This is the authoritative, official U.S. Department of War (DOW) edition of *PRISM: The Journal of Emerging Threats | Complex Statecraft*. Any copyrighted portions of this journal may not be reproduced or extracted without permission of the copyright proprietors. *PRISM* should be acknowledged whenever material is quoted from or based on its content. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of DOW or any other agency of the Federal Government, or any other organization associated with this publication.

3 **Editor-in-Chief's Introduction**

8 **Misleading Orbits: How the Three-Body Problem Distorts Strategic Thought**
By Dr. Todd C. Robinson

23 **Message Resonance Across Cultures: Toward Evidence-based Assessment**
By Dr. Steve S. Sin, Markus K. Binder, and Megan E. Rutter

41 **The Cognitive Domain Is the Main Effort: Why the United States Needs a United States Information Warfare Command**
By Dr. Mason M. Moore

62 **Inside Russia's Proxy Ecosystem: Proxy Curators and Handlers Within the Russian State**
By Eginhards Volāns

82 **Reflexive Control in Financial Markets: Detecting Doctrinal Influence Operations in the Cognitive Battlespace of Global Finance**
By James Tennant and Andrew MacKay

97 **From Ore to Leverage: Lithium, Threat Finance, and Hybrid Competition**
By Bradley A. Mortin

115 **Regulatory Arbitrage and Regional Security Spillovers: Counter-Threat Finance Dynamics in Southeast Asia**
By Dr. Fauzia Gustarina Cempaka Timur, Aulia Akmalina, and Alif Asy'ari

130 **Can the Weak Resist the Strong? Venezuela's Hybrid Asymmetric Options Against U.S. Coercion**
By Jithin Raveendran

149 **The Contested Kinmen Model: Infrastructure as Irregular Warfare in the Taiwan Strait**
By Ian Murphy

168 **Defending with One Hand: How U.S. Cyber Policy Constrains Private Cyber Defense**
By Dr. Mark Grzegorzewski and Tanner Tunstall

183 **Preparing Populations for Hybrid Attacks Against Critical Infrastructure**
By Dr. Heather S. Gregg

197 **The War on Drugs: Insights from the Reagan Era**
By Mark Southern

BOOK REVIEWS

211 **An Extended Review of Three Works on Russian Intelligence and Counterintelligence:**

Counterintelligence at Its Core: Assessing & Preventing Foreign Espionage

The Russian FSB: A Concise History of the Federal Security Service

Tradecraft, Tactics, and Dirty Tricks: Russian Intelligence and Putin's Secret War

Reviewed by Michael W. Parrott

218 **Non-State Special Operations: Capabilities and Effects**

Reviewed by Dr. Kevin D. Stringer

Editor-in-Chief's Introduction

This issue of *PRISM: The Journal of Emerging Threats | Complex Statecraft* examines how adversaries exploit complexity across domains that were once treated as analytically distinct: nuclear strategy, information operations, proxy warfare, financial systems, critical infrastructure, illicit economies, and societal resilience. Taken together, the articles and book reviews in this volume show that irregular warfare is no longer best understood as peripheral to "main" conflict. It is increasingly the grammar through which state and non-state actors compete, coerce, erode, shape, and prepare the strategic environment before—and often instead of—decisive conventional force.

The issue opens with Dr. Todd C. Robinson's "Misleading Orbits: The Problem with the Three-Body Problem," a timely critique of one of the most fashionable metaphors in contemporary strategic discourse. Robinson argues that the now-common analogy between tripolar nuclear competition and the astrophysical three-body problem may appear elegant, but it obscures more than it clarifies. By importing determinism from celestial mechanics into a realm defined by agency, signaling, institutional adaptation, and strategic choice, the metaphor risks hardening a kind of strategic fatalism at precisely the moment policymakers most need conceptual flexibility. His essay is an important reminder that analogies are never neutral. They shape how strategists perceive risk, delimit policy imagination, and decide what forms of adaptation remain possible in an increasingly complex security environment.

From there, Dr. Steve S. Sin, Markus K. Binder, and Megan E. Rutter shift the discussion from strategic metaphor to operational assessment in "Message Resonance Across Cultures: Toward Evidence-based Assessment." Their article tackles a persistent weakness in contemporary information operations: the lack of rigorous tools for judging whether a message will resonate with a target audience before it is deployed. Drawing on a large cross-national dataset across Japan, the Philippines, South Korea, and Taiwan, the authors present the Influence Messaging Impact Model, or IM2, as a more systematic means of evaluating resonance across cultural contexts. Particularly valuable is their effort to move the field beyond surface metrics such as reach and engagement toward deeper variables like value alignment, messenger credibility, narrative coherence, symbolic resonance, and contextual fit. In an issue concerned throughout with cognitive competition, their contribution is foundational: it offers a framework not only for improving friendly information efforts, but also for diagnosing exploitable weaknesses in adversary messaging.

The third article, by Dr. Mason M. Moore, brings the cognitive dimension into direct conversation with institutional reform. In "The Cognitive Domain Is the Main Effort: Why the United States Needs a United States Information Warfare Command," Moore argues that the United States possesses capable information warfare forces but no national architecture for employing them coherently

at the speed and scale demanded by contemporary competition. Comparing the United States unfavorably with China, Russia, Iran, and North Korea, he contends that all of Washington's principal adversaries have already solved the organizational problem of cognitive warfare through centralized command structures, pre-delegated authorities, and integrated narrative architectures. Whether or not readers agree with every element of his proposed United States Information Warfare Command (USIWC), Moore's central point deserves serious engagement: adversaries are treating the cognitive battlespace as a primary theater of competition, while the United States continues to fragment authorities, capabilities, and strategic messaging across bureaucratic seams.

If the first three articles focus on strategic cognition and institutional adaptation, the fourth contribution broadens the aperture to the ecosystemic use of proxies. Inside "Russia's Proxy Ecosystem: Proxy Curators and Handlers Within the Russian State," Eginhards Volāns offers a detailed mapping of the Russian state's orchestration of armed, cyber, and influence proxies. His analysis is especially useful in resisting the temptation to describe Russian proxy warfare as either wholly centralized or wholly improvisational. Instead, Volāns shows a system that is informal, layered, competitive, and increasingly adaptive—one in which the Presidential Administration, GRU, FSB, SVR, *Rosgvardiya,* private military companies, cybercriminal actors, front organizations, and "disposable agents" all interact in ways that both preserve deniability and complicate Western attribution. The article also demonstrates how Russia's proxy apparatus has evolved since the full-scale invasion of Ukraine, including its heavier reliance on looser, more expendable networks recruited through online platforms and intermediaries.

James Tennant and Andrew MacKay then examine another underappreciated battleground in "Reflexive Control in Financial Markets: Detecting Doctrinal Influence Operations in the Cognitive Battlespace of Global Finance." Their essay argues that open societies have invested heavily in offensive financial warfare while doing remarkably little to defend the cognitive integrity of their own markets. Drawing on the Soviet and Russian doctrine of reflexive control, the authors identify patterns by which adversaries may shape investor behavior, induce overreaction, and exploit market narratives without needing to rely on falsehood in the conventional sense. The significance of this article lies in its reframing of financial volatility as not merely a market or regulatory phenomenon, but as an irregular warfare problem. In their telling, capital markets are not just economic mechanisms; they are cognitive terrain, vulnerable to state-linked narrative operations aimed at confidence, timing, and perception.

The next two articles turn explicitly to geoeconomics and illicit finance. In "From Ore to Leverage: Lithium, Threat Finance, and Hybrid Competition," Bradley A. Mortin traces how a critical mineral central to the global energy transition can also become a source of coercion, dependency, and irregular leverage. The article asks readers to think beyond supply-chain disruption in the narrow commercial sense and to recognize how strategic minerals can be folded into threat finance, illicit networks, and coercive statecraft. This is followed by "Regulatory Arbitrage and Regional Security Spillovers: Counter-Threat Finance Dynamics in Southeast Asia," written by Dr. Fauzia Gustarina Cempaka Timur, Aulia Akmalina, and Alif Asy'ari. As a study of regulatory arbitrage, the authors dissect how malign actors exploit jurisdictional seams, legal ambiguities, and compliance gaps to move money, evade scrutiny, and sustain irregular operations. Read together, these essays show that the financial architecture of globalization remains both a source of resilience and a zone of vulnerability. Markets, law, resources, and enforcement regimes are

not peripheral to irregular warfare; they are among its key instruments and targets.

Questions of will, asymmetry, and resistance come to the fore in "Can the Weak Resist the Strong? Venezuela's Hybrid Asymmetric Options Against U.S. Coercion." Jithin Raveendran probes one of the oldest and most consequential questions in irregular warfare: how materially weaker actors endure, adapt, and sometimes prevail against stronger opponents. The essay's value lies in its refusal to romanticize weakness. Resolve alone is insufficient. But the Raveendran shows that social cohesion, strategic clarity, political commitment, and the intelligent use of limited means can transform weakness into a form of leverage. The article resonates with several others in this issue because it treats will not as an abstraction, but as a strategic resource that must be cultivated, protected, and aligned with credible forms of action.

The ninth article, "The Contested Kinmen Model: Infrastructure as Irregular Warfare in the Taiwan Strait," offers one of the issue's clearest illustrations of how infrastructure, dependence, and normalization can be weaponized below the threshold of overt conflict. Focusing on Kinmen, Ian Murphy shows how the People's Republic of China uses water pipelines, proposed energy connections, and other forms of material linkage to cultivate structural dependency and strategic leverage over territory formally controlled by Taiwan. What makes the argument especially compelling is its refusal to separate the physical and cognitive dimensions of coercion. Infrastructure does not merely provide services; it can reshape assumptions, expectations, and political imagination. By normalizing integration through material interdependence, Beijing may be laying the groundwork for forms of control that achieve strategic effect without requiring immediate military occupation. In that sense, the article offers a powerful case study in what might be called geoeconomic encirclement by other means.

That insight carries directly into the article on defending with societal depth rather than with exquisite capability alone. In "Defending with One Hand: How U.S. Cyber Policy Constrains Private Cyber Defense," Dr. Mark Grzegorzewski and Tanner Tunstall argue that many Western states have overinvested in high-end conventional deterrence while underinvesting in the societal resilience needed to withstand long campaigns of disruption, coercion, and ambiguity. This article pairs naturally with Dr. Heather S. Gregg's "Preparing Populations for Hybrid Attacks Against Critical Infrastructure" contribution. Gregg examines how European institutions and selected countries—especially Sweden, the United Kingdom, and Romania—have sought to ready their populations for cyber-enabled disruption, sabotage, and other hybrid attacks on critical goods and services. Her central argument is deceptively simple but strategically profound: when adversaries attack critical infrastructure, the population's reaction is not incidental to the operation; it is part of the intended effect. Panic, distrust, and psychological exhaustion amplify the disruption. Resilience, therefore, is not merely a civil defense matter. It is a frontline requirement of national defense in the era of hybrid threats. Here, resilience is not reduced to emergency stockpiles or infrastructure redundancy. It includes psychological preparation, public trust, civic education, disinformation resistance, and the capacity of institutions and communities to continue functioning under stress. This framing is particularly important because many states still treat civil preparedness as a vestige of an earlier era, rather than as a contemporary requirement of strategic competition.

The issue concludes its article section with Mark Southern's "The War on Drugs: Insights from the Reagan Era," which reframes narcotics trafficking and cartel violence as more than law-enforcement problems. The article argues that contemporary drug networks can function as

irregular threats in their own right and, in some contexts, as semi-proxies that weaken governance, destabilize societies, and complicate U.S. strategic interests. By placing the drug trade within a broader irregular warfare framework, the author pushes readers to think more carefully about the overlap among criminality, sovereignty erosion, border insecurity, corruption, migration pressures, and malign influence. This is a useful corrective to policy conversations that still silo counternarcotics from strategic competition and irregular conflict.

The two book reviews that close the volume complement these themes well. In his extended review essay, Michael W. Parrott surveys three recent works on Russian intelligence and counterintelligence and argues persuasively that intelligence competition is not ancillary to irregular warfare; it is one of its constitutive arenas. By bringing together institutional history, analytic method, and practitioner tradecraft, Parrott highlights how intelligence services shape strategic competition below the threshold of open conflict. The second review, by Dr. Kevin D. Stringer, turns to non-state special operations and the growing capacity of non-state actors to generate strategic effect through precision violence, clandestine organization, and specialized operational methods. Paired together, the reviews underscore an important lesson from this issue as a whole: the shadow battlespace—intelligence, clandestine action, special operations, covert influence, and proxy activity—is not marginal to modern conflict. It is increasingly where the groundwork of larger geopolitical outcomes is laid.

Across these contributions, several common threads emerge. One is that the boundaries separating war and peace, public and private, domestic and foreign, military and civilian, are growing less reliable as organizing categories. Another is that infrastructure—whether digital, financial, maritime, legal, or social—is now a central object of competition. A third is that cognition matters at every level, from how policymakers understand nuclear multipolarity to how populations interpret disruption, fear, authority, and legitimacy. Finally, the issue reminds us that resilience is not a slogan. It is a strategic condition built through institutions, narratives, habits, doctrine, and public trust. Indeed, as several contributors in this issue suggest, the adversary increasingly targets not just militaries, but publics—seeking to exhaust their cohesion, manipulate their perceptions, and reduce their confidence in the state's ability to protect them

For *PRISM*, these themes are entirely in keeping with the journal's mission. Complex operations demand more than tactical adaptation. They require conceptual precision, institutional imagination, and a willingness to engage the uncomfortable reality that adversaries often understand the connective tissue of modern conflict better than we do. The authors in this volume help illuminate that connective tissue. They show how proxies, narratives, infrastructures, legal frameworks, supply chains, and populations interact within a broader field of irregular competition. They also remind us that what appears fragmented at the tactical level may, in strategic terms, be deeply integrated.

That is the challenge before practitioners, scholars, and policymakers alike. If irregular warfare is now a system of systems, then understanding it requires us to resist simplistic metaphors, bureaucratic compartmentalization, and domain stovepipes. It requires seeing that a meme campaign, a pipeline, a lithium concession, a market rumor, a proxy militia, a cyber gang, a public panic, and a doctrine of strategic restraint may all belong to the same competitive ecosystem. While this issue of *PRISM* may not offer an answer to that challenge, it does, however, offer something just as important: a set of rigorous, provocative, and deeply relevant analyses that help us think more clearly about the changing character of complex operations.

Dr. John A. Pennell
Editor-in-Chief

Misleading Orbits

How the Three-Body Problem Distorts Strategic Thought

By Dr. Todd C. Robinson

The past several years has witnessed the rapid diffusion of a new metaphor in U.S. strategic discourse: the three-body problem.[1] Borrowed from classical mechanics, where it denotes the difficulty of predicting the motions of three celestial bodies under mutual gravitational force, the analogy is now regularly invoked to describe a strategic environment in which the United States confronts not one nuclear peer, but two—Russia and China. Among its most prominent advocates was Admiral Charles Richard, former Commander of U.S. Strategic Command, who argued that "there are many passively stable two-body orbital regimes… but there are exactly zero passively stable three-body orbital regimes," suggesting that a tripolar nuclear order is inherently unstable and must be "actively managed."[2] His comments, delivered in multiple public forums, have since been widely referenced in professional discussions of deterrence and nuclear strategy.[3] Others, including former Chairman of the Joint Chiefs of Staff General C. Q. Brown, have also employed the metaphor to describe the current geostrategic environment.[4]

The metaphor's rhetorical power has been amplified by its cultural resonance. The popularization of Liu Cixin's *Three-Body Problem* trilogy, and now its high-profile adaptation as a *Netflix* series, has embedded the term deeply in the broader imagination.[5] As a result, what began as an astrophysical puzzle has migrated into the language of strategic analysis, offering a scientifically inflected shorthand for the challenges of managing great-power nuclear relations in an era of resurgent rivalry.

Yet this essay argues that the metaphor is not only analytically misleading but strategically dangerous. Analogies are never neutral descriptive tools; they structure perception and shape policy responses. Scholars of foreign-policy decision-making have long demonstrated that analogies act as cognitive filters through which policymakers diagnose problems and select strategies.[6] When an analogy imports

Dr. Todd C. Robinson is Associate Professor of Military and Security Studies at SANDS, Air Command and Staff College, Maxwell AFB. He specializes in nuclear strategy, global governance, and institutional design. His work appears in Comparative Strategy, The Nonproliferation Review, Yale Journal of International Affairs, and The National Interest. His co-edited volume, Nuclear Responsibility, was published by Bloomsbury in 2026. He previously served as a Stanton Nuclear Security Fellow at RAND and Associate Director of ACDIS at the University of Illinois, where he earned his PhD.

the wrong assumptions, it distorts more than it clarifies. In the case of the three-body problem, the analogy inaccurately implies that the dynamics of international politics resemble the deterministic, law-bound behavior of celestial bodies. It suggests that strategic actors lack agency, that instability is structurally inevitable, and that collapse is a matter of time unless continuously countered by undefined corrective forces. These implications contradict a central premise of strategic theory: unlike planets governed by Newtonian mechanics, states possess agency, intentionality, and the capacity to adjust behavior through signaling, learning, negotiation, and institutional design.[7]

This matters not only for narrowly understanding nuclear strategy, but also for the broader problem of strategic competition. In contemporary defense discourse, metaphors do not merely describe the environment; they help construct it. They shape how officials frame risk, prioritize capabilities, and imagine what kinds of policy responses are possible. In that sense, the spread of the three-body metaphor is also relevant to the information and cognitive dimensions of competition, including how states think about irregular and hybrid forms of conflict. If strategic communities come to internalize a deterministic image of multipolarity, that image can influence planning, signaling, and perceptions of what forms of restraint or adaptation remain available.

The appeal of the metaphor stems from its elegant simplicity. It imposes a coherent framework on a world increasingly marked by uncertainty: China's rapid military modernization, Russia's coercive nuclear signaling, the erosion of Cold War arms-control architectures, and the diffusion of emerging technologies such as hypersonics and AI-enabled command-and-control systems.[8] But such clarity is purchased at the price of conceptual distortion. By presenting multipolar nuclear politics as a chaotic mechanical system, the metaphor risks undermining strategic imagination. It encourages fatalism, discourages diplomatic innovation, and subtly naturalizes the assumption that instability is unavoidable.

Acknowledging the risks of a tripolar nuclear world is essential, but the conceptual tools we use to understand those risks matter. Strategic metaphors shape the boundaries of policy debate. A metaphor that treats instability as structurally predetermined obscures the political resources available for managing it—crisis-communication mechanisms, arms-control initiatives, declaratory policy adjustments, and norms that shape nuclear restraint. Indeed, the historical record indicates that stability in the nuclear age has always been constructed, not given. The Cold War was not passively stable; it was stabilized through deliberate political choices, institutional innovation, and continual adjustment to perceived risks.[9]

This critique proceeds in seven steps. First, it examines the cognitive role of analogies in strategic thought and highlights their capacity to both illuminate and distort. Second, it explains the actual physics of the three-body problem and how its scientific characteristics have been selectively appropriated in strategic discourse. Third, it contrasts deterministic physical systems with political systems characterized by agency, reflexivity, and interpretation. Fourth, it evaluates the stability of multipolar nuclear orders through both theoretical debates and empirical evidence. Fifth, it interrogates the rise of strategic fatalism in contemporary policy discussions. Sixth, it proposes more suitable conceptual frameworks for understanding strategic complexity. Finally, it concludes by arguing for analytical humility and a renewed commitment to strategic imagination.

At stake is more than the accuracy of a metaphor; it is the mindset through which policymakers conceive the future of nuclear stability. If the strategic community continues to imagine multipolarity

as a gravitational system spiraling toward collapse, it risks overlooking the political tools that can still shape outcomes. Complexity is not chaos, and uncertainty does not negate agency. What the moment demands is not resignation but creativity, and a willingness to think beyond elegant analogies and to build new architectures of stability suited to the emerging nuclear era.

Analogies in Strategic Thought: A Double-Edged Sword

Analogies and metaphors are not merely rhetorical flourishes; they are cognitive instruments that help policymakers navigate uncertainty. Faced with ambiguous information, time pressure, and complex geopolitical dynamics, decision-makers routinely draw on analogical reasoning to make sense of events and identify appropriate responses. As Yuen Foong Khong's seminal work Analogies at War demonstrates, analogical mapping profoundly shapes how leaders diagnose problems, assess causal dynamics, and determine policy options.[10] Yet Khong also shows that analogies can mislead as easily as they can illuminate, especially when policymakers focus on superficial similarities while ignoring deeper structural or contextual differences.

This duality has been explored extensively in the literature on foreign-policy cognition. Robert Jervis, in *Perception and Misperception in International Politics*, argues that analogies help policymakers impose order on a complex reality, but often at the price of distortion.[11] Leaders tend to see what they expect to see and use analogies selectively, reinforcing preexisting beliefs rather than enabling critical reevaluation.[12] Strategic reasoning, therefore, is not solely a function of material conditions; it is shaped by prior expectations, historical memory, and cognitive shortcuts that lend coherence to ambiguous situations.

Analogies in strategic discourse perform several identifiable functions. First, they help construct threat narratives. The Cold War's "domino theory," for instance, offered a visual and intuitive model of sequential state collapse—despite limited empirical support. It framed the geopolitical struggle as a process of contagion, elevating the stakes of local conflicts by situating them within a global, quasi-mechanical process of ideological expansion.[13] Similarly, metaphors such as "tripwires" and "red lines" distill complex strategic concepts into familiar imagery that shapes public and elite perceptions, even when political reality is more nuanced. These analogies are not epiphenomenal; they actively shape how states signal resolve, interpret escalation thresholds, and justify policy choices.

Second, analogies implicitly prescribe policy responses. If a situation is understood as "another Munich," appeasement becomes unacceptable and military firmness appears necessary. If it is "another Vietnam," restraint and disengagement gain rhetorical force. The analogy thus serves as a template for action. As Jervis notes, the danger is that the analogy may obscure disconfirming evidence or alternative interpretations, narrowing the range of options considered.[14]

The "three-body problem" metaphor functions differently from historical analogies like Munich or Vietnam. Rather than invoking past strategic failures, it draws its authority from the perceived objectivity of science. By mapping geopolitical dynamics onto the deterministic mechanics of gravitational interaction, it conveys an impression of analytical precision and inevitability. The metaphor suggests that great-power nuclear relations resemble a mechanically unstable physical system—one in which equilibrium is fleeting, feedback loops are uncontrollable, and chaos is structurally embedded. This framing grants the analogy a veneer of scientific legitimacy that is especially seductive in policy debates seeking clarity amid uncertainty.

But this is precisely where the analogy becomes perilous. Physics operates within a domain governed by immutable laws, whereas international politics operates within a domain defined by agency, interpretation, and choice. Celestial bodies cannot reassess intentions, engage in backchannel diplomacy, or modify trajectories based on reciprocal signaling. States can. By importing a deterministic model from astrophysics into strategic thought, the analogy risks naturalizing instability and depriving policymakers of the intellectual space necessary to imagine alternative futures.

Strategic analogies can also become self-fulfilling. If leaders internalize the idea that a tripolar nuclear world is inherently unstable, they may adopt policies—such as worst-case planning, arms racing, or resistance to transparency—that increase the very risks the analogy purports to describe. As constructivist scholars have shown, ideas and expectations shape behavior; they are not passive reflections of material structure.[15] A metaphor that depicts instability as unavoidable encourages fatalistic strategies that crowd out diplomatic innovation.

This is especially important in an era in which strategic competition increasingly unfolds through contests over interpretation, narrative, and framing. The concepts that circulate through defense institutions do not remain confined to academic debate; they shape planning assumptions, bureaucratic priorities, and the language through which policymakers communicate with allies and adversaries alike. In that sense, strategic metaphors operate within the cognitive dimension of competition. They are part of how states define what kind of problem they believe they are confronting in the first place.

To evaluate analogies systematically, scholars have proposed criteria that distinguish illuminating comparisons from misleading ones. A sound strategic analogy should display meaningful structural similarity, causal equivalence, and temporal comparability between the source domain and the target domain. It should also generate useful insights for action rather than foreclose the policy space.[16] The three-body analogy fails these tests. While it captures the increased complexity of a tripolar system, it does so at the cost of ignoring core features of international politics—agency, reflexivity, signaling, and institutional adaptation. These are not peripheral aspects; they are the foundation of strategic interaction in the nuclear age.[17]

In sum, analogies are powerful cognitive tools that must be handled with care. They simplify complexity, but simplification inevitably excludes. The danger arises when an analogy is elevated to the status of a model—when its limitations fade from view and its assumptions silently dictate strategic thought. The growing prominence of the three-body problem metaphor represents precisely this risk. Before it becomes a dominant conceptual frame in policy discourse, it requires rigorous scrutiny. Without such scrutiny, an elegant scientific metaphor may quietly harden into a strategic worldview—one that obscures agency, promotes fatalism, and constrains the very creativity needed to manage nuclear multipolarity.

The Physics of the Three-Body Problem

The "three-body problem" holds a distinctive place in the history of classical mechanics. First formulated by Isaac Newton in the *Principia*, the problem concerns predicting the motion of three celestial bodies interacting through mutual gravitational force. While Newton was able to derive exact, closed-form solutions for the two-body problem—epitomized by the orderly motion of planets around the sun—he quickly recognized that the addition of even a third body renders the system analytically intractable.[18] The interactions among three bodies produce nonlinear feedback loops that resist simplification, and by the 19th century the three-body

problem had become one of the classic demonstrations of deterministic chaos.[19]

Henri Poincaré's groundbreaking work in the 1890s revealed why the three-body system behaves so unpredictably. He showed that tiny differences in initial conditions—position, velocity, mass ratios—can lead to dramatically divergent trajectories, producing what is now commonly described as sensitive dependence on initial conditions.[20] This insight laid the conceptual foundation for modern chaos theory. The central problem is that each body influences, and is influenced by, the others simultaneously; the gravitational pull is never constant, and no force remains independent of the system's evolving configuration. The result is a dynamic that is not merely complex but structurally unstable.

To illustrate: inserting a third mass into an otherwise stable two-body orbit destabilizes the equilibrium. The newcomer disrupts gravitational balance, altering the trajectories of the original pair, which in turn modifies the motion of the third. Even minute differences can accumulate over time until the system appears chaotic oscillating unpredictably, entering erratic resonance patterns, or ejecting a body entirely. While physicists have identified certain special configurations that yield quasi-stable behavior—such as the Lagrange points in the Earth–Moon–Sun system—these arrangements are rare, fine-tuned, and easily perturbed.[21]

It is this scientific narrative of structural instability that has proven attractive to strategic thinkers. Admiral Charles Richard's invocation of the three-body problem explicitly draws on the notion that while two-body systems exhibit "passive stability," three-body systems do not. His conclusion, widely quoted, is that a tripolar nuclear world is inherently unstable unless subjected to "active stabilization," though what such stabilization would entail remains unclear in practice.[22]

At first glance, the metaphor seems compelling. Just as a third celestial body disrupts gravitational equilibrium, the emergence of China as a major nuclear power alongside the United States and Russia appears to complicate deterrence relationships. Each state influences the security calculations of the others, producing new feedback loops, untested combinations of signaling, and the potential for cascading escalation. The metaphor's intuitive appeal lies in its promise to explain a complex strategic environment through a familiar scientific framework.

But this is where the analogy begins to mislead. The three-body problem's behavior is governed by immutable physical laws: masses, distances, and gravitational constants. The bodies cannot learn, anticipate, or communicate. Their trajectories are dictated entirely by initial conditions and the deterministic equations of motion. In contrast, international politics operates in a domain shaped by agency, intention, perception, and reflexivity. States do not move through the strategic landscape as inert objects pulled by impersonal forces. They learn, adapt, negotiate, misinterpret, and recalibrate. Their behavior is not predetermined by structure but shaped through continual assessment and reinterpretation of others' actions.[23]

The analogy also obscures a crucial difference regarding feedback. In celestial mechanics, feedback loops arise automatically from physical laws; bodies influence each other regardless of intent. In nuclear strategy, feedback loops emerge through signaling, doctrine, posture, and interpretation—processes mediated by human judgment and political institutions. Misperceptions can amplify risk, but clarity, communication, and restraint can mitigate it. The system is not mechanically unstable; its stability is contingent, socially constructed, and politically managed.[24]

Furthermore, political systems are open, not closed, as physical systems are assumed to be for the purposes of modeling. New actors can emerge (e.g., India's expanding nuclear capabilities), technologies

can disrupt established patterns (e.g., AI-enabled early warning, hypersonic weapons), and internal political changes can alter strategic preferences. Celestial bodies do not change their mass or trajectory voluntarily; states can and do, sometimes rapidly. This fluidity fundamentally breaks the deterministic parallel that the three-body metaphor seeks to establish.

In strategic discourse, the metaphor's deterministic overtones can inadvertently promote a vision of inevitability—a belief that instability is "baked in" to a tripolar nuclear order. If taken seriously, this worldview encourages strategic fatalism: policymakers may assume that arms-control arrangements are futile, that crisis communication cannot meaningfully reduce risk, or that military modernization is the only plausible path to maintain stability. As scholars of deterrence and nuclear politics have long argued, such fatalism is itself dangerous because it becomes self-reinforcing.[25]

In sum, while the three-body problem is scientifically elegant and genuinely captures the mathematical difficulty of predicting multibody gravitational systems, it fails as an analogy for nuclear multipolarity. It imports assumptions—determinism, lack of agency, closed-system dynamics—that are incompatible with the essence of international politics. Its use in strategic thought may simplify complexity, but it does so at the cost of distorting the domain it purports to illuminate.

From Physics to Politics: Agency in Strategic Systems

The movement from celestial mechanics to geopolitical strategy is not just a metaphorical leap; it is a transition across fundamentally incompatible domains of causality. In physics, especially in the context of the three-body problem, objects obey deterministic laws. Their trajectories are fully dictated by mass, distance, and gravitation. They possess no capacity for foresight, no ability to interpret signals, and no mechanism for revising behavior based on learning or experience. They simply respond to forces acting upon them. This is the essential premise of Newtonian mechanics.[26]

International politics operates on entirely different principles. States are not celestial bodies; they are agents embedded in complex social environments. They possess political leadership, organizational structures, strategic cultures, and domestic constituencies. They interpret, anticipate, misperceive, negotiate, and adapt. Their actions emerge not from mechanical inevitabilities but from political choice and strategic interaction.[27] This distinction is not academic; it is foundational. The very concept of strategy presupposes agency. To treat states as planets is to erase the core features of political life.

This difference is especially clear in nuclear politics, where signaling, credibility, and perception shape outcomes as much as—if not more than—material capabilities. Consider the Cuban Missile Crisis, widely studied as the most dangerous nuclear confrontation in history. Had the United States and the Soviet Union behaved like gravitational bodies, their relative power and initial trajectories would have dictated the outcome. Instead, leaders on both sides engaged in deliberate acts of escalation management: public and private signaling, backchannel communication, careful calibration of military posture, and ultimately reciprocal concessions.[28] Catastrophe was avoided not because the system found an equilibrium on its own, but because political actors exercised judgment within a fluid, high-risk environment.

This example underscores a broader point: international systems are reflexive. Actors behave based on beliefs about how others will behave—a dynamic with no analogue in the physical sciences.[29] If China anticipates that U.S. policy is trending toward containment, it may harden its strategic posture; if the United States interprets that hardening as aggression, it may respond in kind. These

feedback loops are constructed through perception, not gravity. The system is therefore not deterministic but socially generated, meaning instability is not dictated by structure alone but shaped by evolving expectations and interpretations.

The presence of norms and institutions further distances international politics from physical models. Treaties, regimes, and informal understandings constrain behavior despite lacking deterministic force. The Non-Proliferation Treaty (NPT), for example, is a legal framework whose effectiveness stems from normative legitimacy as much as enforcement. Similarly, the longstanding "nuclear taboo," as argued by Nina Tannenwald, has contributed to the non-use of nuclear weapons since 1945 not simply because of fear of retaliation, but because the idea of nuclear use has become morally and politically stigmatized.[30] Nothing in celestial mechanics resembles such ideational constraints.

Another flaw in the three-body analogy lies in its assumption of a closed system. In physics, the three-body problem includes no external actors, no technological change, and no internal transformation of the bodies themselves. International politics is the opposite: systems are open, dynamic, and subject to internal and external shocks. New actors emerge—India, Pakistan, and North Korea each altered the global nuclear landscape at various moments. Technologies evolve, creating new domains of vulnerability and new pathways for escalation, such as cyber intrusion into command-and-control systems or AI-enhanced early warning. Domestic political changes can suddenly transform national preferences, as seen in Iran's nuclear trajectory across administrations or Russia's shifting strategic posture under Vladimir Putin.

Such transformations are not only possible; they are routine. This fluidity breaks the deterministic equivalence that the three-body analogy presumes. In geopolitical systems, the identities, preferences, and capabilities of actors evolve over time. This means that stability is not a function of structural configuration alone; it is a product of political management, institutional design, and strategic dialogue.[31]

Agency also implies the possibility of restraint—an option nonexistent in physical systems. During the Cold War, both the United States and the Soviet Union deliberately adopted measures to stabilize the nuclear competition: arms-control treaties, hotlines, risk-reduction centers, crisis protocols, and doctrinal adjustments. These were not gravitationally induced equilibria, but intentionally constructed guardrails built through diplomacy and negotiation.[32] The fact that the nuclear order endured for decades without catastrophic failure is evidence that agency, not structure, defines strategic outcomes.

This point bears directly on contemporary debates about nuclear multipolarity. If one adopts the deterministic worldview implied by the three-body analogy, the conclusion is that instability in a U.S.–China–Russia system is inevitable. But this is a conceptual error. The tripolar system is not a mechanical system tending toward chaos; it is a political system whose stability depends on choices yet to be made. Whether it becomes more dangerous or more stable is not predetermined by "gravitational" dynamics but will be shaped by diplomacy, signaling practices, decision-making processes, and institutional innovation.

In short, physics teaches that three-body systems lack passive stability. Politics teaches that stability is never passive to begin with; it is constructed. Treating states as celestial bodies obscures their ability to build order, manage risk, and create mechanisms that prevent catastrophe. Instability in international politics is not a law of nature. It is a challenge for strategy.

Strategic Stability in a Multipolar Nuclear World

If the three-body metaphor fails to capture the essential features of political agency, then the next

question is analytical rather than rhetorical: what does strategic stability actually look like in a world where three major nuclear powers coexist? Does the transition from bipolarity to multipolarity necessarily undermine stability, or is this conclusion itself a byproduct of misleading analogical reasoning?

Bipolarity as a Strategic Ideal? Revisiting Waltz

Kenneth Waltz's structural realism has had a profound influence on nuclear strategy debates. Waltz famously argued that bipolar systems are the most stable because they simplify threat assessment and reduce the risk of entanglement. In such a system, each pole primarily balances the other, making miscalculation less likely and crisis dynamics more predictable.[33] For many observers, the Cold War appeared to validate this logic: despite moments of extreme tension, the United States and the Soviet Union avoided direct war, and nuclear deterrence remained intact.

Waltz extended this reasoning into nuclear theory, arguing controversially that nuclear weapons can introduce stability even in multipolar regions, so long as states possess secure second-strike capabilities and behave rationally.[34] But Waltz's framework has two limitations. First, it lacks a clear definition of "stability." Is stability the absence of great-power war, the absence of arms racing, or the predictability of crisis behavior? Without clarity, the argument risks circularity: bipolarity is stable because it is bipolar.

Second, Waltz's account minimizes the role of perceptions, signaling, miscalculation, and domestic politics. These so-called "unit-level variables" are not peripheral noise; they are central to nuclear dynamics. As decades of research show, states frequently misinterpret adversaries' intentions, make erroneous assumptions about resolve, or fail to anticipate political pressures that shape decision-making.[35] The Cold War was not stable because of structure alone—it was stabilized through diplomacy, crisis management, doctrinal innovation, and luck.

Is Multipolarity Inherently More Dangerous?

As China expands and modernizes its nuclear arsenal, joining the United States and Russia as a nuclear peer competitor, analysts have increasingly warned that we are entering uncharted and unstable strategic terrain. Admiral Richard's assertion that "we have never faced two nuclear peer competitors" captures this concern and has been echoed widely in strategic commentary.[36] The implicit claim is that a tripolar nuclear system resembles a three-body gravitational system: inherently unstable, prone to cascading effects, and difficult to manage.

But this conclusion is not grounded in theory or evidence. It is grounded in analogy. The historical and empirical record is far more nuanced.

During the Cold War, the United States already navigated a quasi-multipolar environment involving independent British, French, and Chinese nuclear forces. None of these additional nuclear actors destabilized the global deterrence system in a manner consistent with predictions derived from the three-body metaphor. Their arsenals introduced complexity, but not chaos. The fact that the United States and Soviet Union retained preponderant capabilities mattered, but it was political management—not gravitational determinism—that preserved stability.[37]

Similarly, in South Asia, the India–Pakistan nuclear rivalry—often cited as an inherently unstable dyad—has thus far produced repeated crises but no full-scale war since both states achieved overt nuclear status. Nuclear weapons have constrained escalation even amid dangerous political shocks.[38] This is not evidence of mechanical stability; it is evidence that agency and learning shape deterrence outcomes.

Stability as a Constructed Outcome

An emerging body of scholarship emphasizes that strategic stability is not a property of system structure but a constructed outcome.[39] Stability emerges from shared expectations, mutual restraint, institutional arrangements, and tacit or explicit communication. It is a social product, not a mechanical one.[40]

The nuclear taboo, for example, is a normative constraint that has helped shape state behavior for decades. Its origins are not found in deterrence logic alone; they are rooted in evolving moral, political, and legal norms surrounding the use of nuclear weapons.[41] In a multipolar world, such norms—alongside emerging ones governing cyber operations, autonomous systems, and space conflict—will be critical to mitigating escalation risks.

If stability is constructed, not given, then multipolarity is not inherently unstable. It is simply more demanding. The absence of trilateral arms-control agreements among the United States, Russia, and China is problematic not because multipolarity is unmanageable, but because the political mechanisms for constructing stability are underdeveloped.

Complexity Is Not Chaos

Multipolarity introduces new pathways for misinterpretation and escalation. Each state must consider interactions not only with adversaries, but also with third parties whose responses may be unpredictable. Yet more actors also introduce more opportunities for communication, redundancy, and restraint. Complexity increases the number of potential failure points, but it also increases the number of possible stabilizing arrangements. As work in complex systems theory shows, multi-actor environments do not automatically degrade into chaos; they can exhibit emergent forms of order if actors adjust to feedback and learn over time.[42]

Political choice, not structural determinism, drives this adaptive process.

Strategic Fatalism as a Policy Choice

The greatest danger of the three-body analogy is not analytical; it is psychological. If policymakers believe that a multipolar nuclear world is inherently unstable, they may deprioritize diplomacy, assume worst-case intentions, and resist arms-control initiatives on the grounds that they cannot meaningfully alter system dynamics. This fatalism becomes self-reinforcing, raising the very risks it seeks to mitigate.

But instability is not destiny. The future of great-power nuclear relations will depend on whether states adopt strategies that reduce uncertainty, enhance transparency, and institutionalize communication. Arms control, crisis hotlines, military-to-military dialogues, AI-governance frameworks, and confidence-building measures are not relics of a bygone bipolar order—they are necessary foundations for stability in a more complex nuclear environment.

In short, multipolarity is not the problem. The problem is assuming that multipolarity is unmanageable.

Better Models, Better Metaphors

If the three-body problem is an analytically flawed and strategically counterproductive metaphor, the appropriate response is not to abandon metaphor altogether. Strategic thought depends on simplification; complexity must be rendered legible to become actionable. The challenge is to employ metaphors and models that illuminate rather than obscure—those that preserve agency, allow for institutional adaptation, and capture the dynamic, socially constructed nature of international politics.

Several alternative frameworks offer more accurate and intellectually productive ways to

conceptualize strategic interaction in a multipolar nuclear world.

1. The Complex Adaptive System

One promising approach draws from complexity science and views the international system as a complex adaptive system (CAS). In this framework, states are not inert bodies governed by external forces but adaptive agents capable of learning, modifying behavior, and altering their environment.[43] Feedback loops exist in CAS models, but they do not produce deterministic collapse. Instead, system-wide patterns emerge from the interactions of adaptive actors. Order and stability are not assumed; they are produced through iterative adjustment.

This framework better captures the nature of contemporary nuclear dynamics. States observe each other's behavior, revise threat assessments, engage in signaling, adopt confidence-building measures, and develop institutional mechanisms to constrain risk. These adaptive processes have no equivalent in celestial mechanics but are central to nuclear strategy. Focusing on adaptation rather than determinism encourages analysts to explore how stability can emerge—not automatically, but through purposeful political action.

2. Iterated Strategic Interaction: Lessons from Game Theory

Game theory offers another metaphor that is more faithful to the political domain: iterated strategic games. Unlike single-shot interactions, iterated games highlight the importance of repeated interaction, learning, and reciprocity. Robert Axelrod's work on the iterated Prisoner's Dilemma demonstrated that cooperative strategies such as "tit for tat" can produce stable outcomes over time, even when defection appears rational in a single round.[44]

Applied to nuclear multipolarity, an iterated-games metaphor suggests that states can develop stable patterns of behavior through repeated signaling, reciprocal restraint, and the institutionalization of norms. Strategic stability becomes a function not of structural configuration but of expectations and practices generated through ongoing interaction. This perspective foregrounds agency and learning—two dimensions absent from the three-body analogy but essential to nuclear deterrence.[45]

3. Ecological Models: Resilience, Not Equilibrium

Ecological metaphors offer a third alternative. In ecology, stability does not mean the absence of shocks; it means the capacity of a system to absorb shocks without collapsing. This notion of resilience provides a richer way to conceptualize nuclear stability. In an ecological system, different species coexist through processes of adaptation, feedback, and niche differentiation. Disturbances are expected, but systems can reorganize and persist.

Translating this insight into international politics suggests that we should think less in terms of equilibrium—a concept borrowed from mechanics—and more in terms of resilience. A resilient nuclear order is one that can withstand crises, technological disruptions, and political shocks without escalating to nuclear use. Norms such as the nuclear taboo, institutional frameworks like arms-control agreements, and informal understanding of thresholds all contribute to systemic resilience.[46] This model acknowledges complexity without succumbing to fatalism.

4. Models That Preserve Strategy

What unites these alternative metaphors is that they preserve the possibility of strategy. They do not assume that system dynamics are predeter-

mined. They do not portray instability as an immutable law. Instead, they highlight mechanisms such as learning, adaptation, communication, and institution-building through which political actors can influence outcomes.

These models also acknowledge uncertainty, but they treat it as an opportunity for innovation rather than an argument for resignation. That framing matters. As Thomas Schelling emphasized, strategy is fundamentally an interactive process: what matters is not just what states do, but how they expect others to respond.[47] Metaphors that deny agency deny the very premise of strategy.

Models Are Not Truths—They Are Tools

A crucial point must be underscored: metaphors and models do not describe reality; they help us reason about it. The question is not whether a metaphor is perfectly accurate - it never is - but whether it aids analysis and expands the range of policy options. The three-body metaphor fails this test. It offers elegance at the cost of agency, and determinism at the cost of imagination.

By contrast, CAS models, iterated games, and ecological frameworks emphasize:

- that strategic behavior is shaped by interaction, not structure alone;
- that norms and institutions matter;
- that uncertainty is manageable;
- and that stability must be constructed, not assumed.

These models do not deny the risks of nuclear multipolarity. Rather, they provide conceptual space for strategies that can mitigate those risks. They encourage policymakers to envision new architectures of stability suited to a world no longer defined by Cold War bipolarity.

Toward a More Imaginative Strategic Vocabulary

The future will demand metaphors that broaden, rather than narrow, strategic thought. The United States, China, and Russia are entering a dangerous period, but danger does not eliminate agency. By adopting metaphors that capture the adaptive, interactive, and socially constructed nature of nuclear politics, scholars and policymakers can avoid the fatalism inherent in deterministic frameworks and instead cultivate a strategic vocabulary that supports innovation.

Ultimately, the goal is not to find a single perfect metaphor. It is to ensure that our conceptual tools expand rather than constrain the space for policy imagination.

Policy Implications: Avoiding Metaphor-Driven Fatalism

If the "three-body problem" is a poor guide to strategy, the practical question is what should replace it. The answer is not a new predictive model, but a shift in how policymakers frame the problem itself. Strategic competition in a multipolar nuclear environment is better understood as a problem of political management rather than mechanical instability. That distinction matters. If policymakers assume the system is inherently chaotic, they are more likely to default toward worst-case planning, arms racing, and skepticism about diplomacy. If instability is instead understood as contingent, shaped by interpretation, signaling, and institutional design, then policy space reopens.[48]

The first implication is that "active management" should not be treated as synonymous with military buildup. Much of the current discourse collapses management into more capabilities, higher readiness, and more visible demonstrations of resolve. Some of this may be necessary. But stability

has never depended on force posture alone. It has also depended on whether states can make their behavior legible to one another and reduce the risk that routine competition is misread as preparation for escalation. A strategy focused narrowly on capability risks producing a more heavily armed but less intelligible strategic environment.[49]

A second implication is the need to rebuild what might be called interpretive infrastructure. During the Cold War, stability was reinforced through signaling practices, hotlines, arms-control efforts, and shared understandings about what certain actions were meant to communicate. Much of that infrastructure has weakened, and no equivalent exists for a triangular nuclear relationship involving the United States, Russia, and China. The priority, therefore, is not to "solve" multipolarity, but to expand the channels through which intentions, thresholds, and patterns of behavior can become more intelligible over time. Contemporary defense guidance increasingly recognizes this challenge. The *Joint Concept for Competing* emphasizes the importance of narrative, framing, and decision advantage in shaping strategic outcomes; an implicit acknowledgment that how actors interpret the environment is itself a domain of competition.[50]

This challenge is magnified by the cross-domain character of contemporary competition. Strategic interaction now unfolds across cyber operations, space systems, and conventional capabilities that can shape nuclear perceptions without being nuclear in form. The problem is not simply deterrence, but misinterpretation across domains. Recent scholarship on escalation risks highlights how entanglement between nuclear and non-nuclear systems can create pathways for inadvertent escalation driven by perception rather than intent.[51] Policies that reduce ambiguity, particularly where non-nuclear actions may be read as threatening strategic deterrents, are therefore central to stability.

A third implication is that policymakers should be more disciplined in how they use metaphor itself. Metaphors are unavoidable, but they should function as heuristics rather than models. Useful metaphors preserve agency, allow for learning, and leave room for institutional innovation. Dangerous ones imply inevitability and narrow the perceived range of options. The risk of the three-body analogy is not that it is vivid, but that it encourages the belief that instability must be endured rather than managed.[52]

Multipolarity undoubtedly introduces new complications. But complexity is not impossibility. The greater danger lies in approaching a more complex environment with conceptual tools that encourage fatalism instead of adaptation. The task is not to recreate bipolar stability under more difficult conditions, nor to accept instability as given. It is to build new practices, expectations, and institutions capable of sustaining restraint under different strategic conditions.

For policymakers, the lesson is straightforward: the problem is not that the strategic environment has become too complex to manage. The problem is that poor conceptual framing can make it harder to see what management requires. A better strategic vocabulary will not eliminate risk, but it can help ensure that uncertainty is not mistaken for inevitability.

Conclusion: Strategy Requires Imagination

In an era defined by resurgent great-power rivalry, accelerating technological disruption, and the erosion of long-standing arms-control regimes, the search for conceptual clarity is understandable. Strategic environments marked by uncertainty naturally invite metaphors that offer coherence and predictive power. The "three-body problem," with its scientific pedigree and elegant formulation, has therefore gained rapid traction as a way of describing the emerging nuclear order. Yet as this

essay has argued, the metaphor fails on analytical, theoretical, and strategic grounds.

The analogy's appeal lies in its simplicity, but that simplicity is bought at the cost of accuracy. By importing deterministic notions of instability from celestial mechanics into international politics, the three-body metaphor obscures the fundamental drivers of strategic behavior—agency, interpretation, signaling, institutional design, and adaptive learning. It suggests that instability in a tripolar nuclear world is structurally inevitable, when in fact history shows that stability has never been passive. It has always been constructed.

The Cold War did not remain peaceful because two superpowers happened to exist in a stable configuration. Stability emerged through the creation of crisis hotlines, arms-control agreements, mutual understandings about thresholds, doctrinal innovation, and the development of shared norms, including the moral and political taboo against nuclear use.[53] These stabilizing mechanisms were products of deliberate political choice—not gravitational inevitability.

The danger of adopting the three-body metaphor uncritically is not merely analytical. It is psychological and political. Deterministic metaphors encourage deterministic thinking. If policymakers internalize the belief that multipolarity is inherently unstable and destined to collapse, they may behave in ways that accelerate arms racing, undermine diplomacy, and normalize worst-case planning. Strategic fatalism becomes a self-fulfilling prophecy. The metaphor that was intended to clarify instead constrains, limiting the strategic imagination at precisely the moment when imagination is most needed.

Rejecting the three-body analogy does not require denying the risks of nuclear multipolarity. Those risks are real and growing. But risk is not destiny. The emerging nuclear environment demands frameworks that capture complexity without sacrificing agency, that acknowledge uncertainty without surrendering to fatalism. Models drawn from complex adaptive systems, iterated strategic interaction, and ecological resilience offer more productive ways to conceptualize the challenges ahead—models that highlight the possibility of learning, mutual restraint, and institutional innovation.[54]

The choice of metaphor matters because metaphors define the boundaries of the thinkable. A metaphor that depicts the strategic future as a chaotic, collapsing system narrows those boundaries. It replaces strategy with resignation. By contrast, metaphors that foreground agency, adaptation, and resilience expand the horizons of possibility. They invite policymakers to conceive of emerging nuclear dynamics not as an astrophysical puzzle to be endured, but as a political challenge to be managed.

As the United States, China, and Russia navigate the most complex strategic environment since the height of the Cold War, the task is not to solve the three-body problem. It is to remember that we are not celestial bodies. We are political actors with the ability, and responsibility, to shape the contours of stability through diplomacy, communication, restraint, and institution-building. In the end, as Clausewitz reminds us, strategy is not a science governed by immutable laws. It is an art conducted amid uncertainty.[55] That art begins with imagination. And imagination is shaped by the metaphors we choose. Choosing the wrong metaphor can quietly prepare us for catastrophe. Choosing the right one may help us prevent it.

Endnotes

[1] Henri Poincaré, "Sur le problème des trois corps et les équations de la dynamique," *Acta Mathematica* 13 (1890): 5–6, 67–70.
[2] Charles A. Richard, public remarks as Commander, U.S. Strategic Command, to the 2021 Space and Missile Defense Symposium.
[3] Charles A. Richard, public remarks as Commander, U.S. Strategic Command, to the 2021 Space and Missile Defense Symposium.
[4] C. Q. Brown, public remarks as Chairman, US Joint Chiefs of Staff, to the 2024 STRATCOM Deterrence Symposium. https://www.youtube.com/watch?v=Py38eaA-j0Zc Accessed on February 4, 2025.
[5] Liu Cixin, *The Three-Body Problem* (Chongqing: Chongqing Press, 2008); *3 Body Problem*, Netflix television series, created by David Benioff, D. B. Weiss, and Alexander Woo, released March 2024.
[6] Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ: Princeton University Press, 1992); Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).
[7] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (New York: Columbia University Press, 1977).
[8] Nina Tannenwald, "The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use," *International Organization* 53, no. 3 (1999): 433–468; Scott D. Sagan and Kenneth N. Waltz, *The Spread of Nuclear Weapons: A Debate Renewed*, 2nd ed. (New York: W. W. Norton, 2002).
[9] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976); Thomas C. Schelling, *Arms and Influence*.
[10] Khong, *Analogies at War*.
[11] Jervis, *Perception and Misperception in International Politics*, 117-120.
[12] Ibid.
[13] Khong, *Analogies at War*.
[14] Jervis, *Perception and Misperception in International Politics*, 121-123.
[15] Tannenwald, *The Nuclear Taboo*.
[16] Khong, *Analogies at War*; Jervis, *Perception and Misperception in International Politics*.
[17] Schelling, *Arms and Influence*; Bull, *The Anarchical Society*.
[18] Isaac Newton, *The Principia: Mathematical Principles of Natural Philosophy*, trans. I. Bernard Cohen and Anne Whitman (Berkeley: University of California Press, 1999), bk. I. (Original work published 1687).
[19] Henri Poincaré, "Sur le problème des trois corps et les équations de la dynamique," *Acta Mathematica* 13 (1890): 5–6, 67–70.
[20] Ibid, 1 –6, 67–70.
[21] Victor Szebehely, *Theory of Orbits: The Restricted Problem of Three Bodies* (New York: Academic Press, 1967).
[22] Charles A. Richard, public remarks as Commander, U.S. Strategic Command, including the 2021 Space and Missile Defense Symposium.
[23] Schelling, *Arms and Influence*; Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989).
[24] Bull, *The Anarchical Society*; Tannenwald, *The Nuclear Taboo*.
[25] Sagan and Walz, *The Spread of Nuclear Weapons: A Debate*.
[26] Isaac Newton, *The Principia: Mathematical Principles of Natural Philosophy*, trans. I. Bernard Cohen and Anne Whitman (Berkeley: University of California Press, 1999), bk. I. (Original work published 1687).
[27] Schelling, *Arms and Influence*; Jervis, *Perception and Misperception*.
[28] Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown and Company, 1971); Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974).
[29] Jervis, *Perception and Misperception in International Politics*.
[30] Tannenwald, *The Nuclear Taboo*.
[31] Bull, *The Anarchical Society*; Ulrich Kühn, "Strategic Stability in the 21st Century: An Introduction," *Journal of Strategic Studies* 46, no. 3 (2023).
[32] Schelling, *Arms and Influence*, Jervis, *Perception and Misperception in International Politics*.
[33] Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979).
[34] Sagan and Waltz, *The Spread of Nuclear Weapons: A Debate*.
[35] Jervis, *Perception and Misperception In International Politics*; Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981).
[36] Charles A. Richard, public remarks as Commander, U.S. Strategic Command, to the 2021 Space and Missile Defense Symposium.

[37] John Lewis Gaddis, *The Long Peace: Inquiries into the History of the Cold War* (New York: Oxford University Press, 1987).
[38] Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton, NJ: Princeton University Press, 2014).
[39] Kühn, U. (2023). "Strategic Stability in the 21st Century: An Introduction." *Journal for Peace and Nuclear Disarmament*, *6*(1), 1–8.; Onderco, M. (2025). "Nuclear regime complex and state relations in nuclear ordering." *Cambridge Review of International Affairs*, *38*(3), 302–318.
[40] Bull, *The Anarchical Society*.
[41] Tannenwald, *The Nuclear Taboo*.
[42] Robert Axelrod and Michael D. Cohen, *Harnessing Complexity: Organizational Implications of a Scientific Frontier* (New York: Free Press, 1999).
[43] Ibid.
[44] Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984).
[45] Schelling, *Arms and Influence*.
[46] Tannenwald, *The Nuclear Taboo*; Bull, *The Anarchical Society*.
[47] Schelling, *Arms and Influence*.
[48] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).
[49] Schelling, *Arms and Influence*; Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (New York: Columbia University Press, 1977).
[50] U.S. Department of Defense, *Joint Concept for Competing* (Washington, DC: Department of Defense, 2023).
[51] James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (2018): 56–99; Fiona S. Cunningham and M. Taylor Fravel, "Dangerous Confidence? Chinese Views on Nuclear Escalation," *International Security* 44, no. 2 (2019): 61–109.
[52] Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ: Princeton University Press, 1992); Jervis, *Perception and Misperception in International Politics*.
[53] Tannenwald, *The Nuclear Taboo*; Bull, *The Anarchical Society*.
[54] Axelrod and Cohen, *Harnessing Complexity*; Axelrod, *The Evolution of Cooperation*.
[55] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), bk. I, chap. 1.

Message Resonance Across Cultures

Toward Evidence-based Assessment

By Dr. Steve S. Sin, Markus K. Binder, and Megan E. Rutter

Introduction

American military organizations operate in modern information environments without validated frameworks for evaluating message resonance with target audiences. This assessment deficit creates two distinct operational problems. First, organizations deploying information campaigns cannot predict whether messages will achieve intended effects. This generates risk of iatrogenic outcomes—well-intentioned communications that end up contradicting strategic objectives. Second, when confronting adversarial information campaigns, organizations lack systematic methodology for identifying exploitable message weaknesses. Current practice emphasizes content moderation, platform manipulation detection, and reactive rebuttal. These approaches fail to exploit structural vulnerabilities in adversarial messaging, representing a significant gap in operational capability that demands doctrinal and methodological development.

Steve S. Sin, Ph.D. is an associate research scientist and director of the Unconventional & Asymmetric Threats Division at START, University of Maryland. His research spans adversary behavior modeling, multi-domain operations, emerging technologies, and countering weapons of mass destruction. He leads interdisciplinary programs funded by DOW, DHS, and others. He previously served as senior research associate at the National Center for Security & Preparedness and as a U.S. Army officer.

Markus K. Binder is a principal faculty specialist at START, University of Maryland. His research focuses on adversary behavior modeling and countering weapons of mass destruction, particularly why certain actors pursue or employ CBRN capabilities while others do not. He serves as co-principal investigator and project manager on several unconventional threats projects and manages multiple databases tracking global CBRN weapon use by violent non-state and criminal actors.

Megan E. Rutter is a senior faculty specialist at START, University of Maryland. Her expertise spans international security and counterterrorism. She serves as research staff on projects addressing irregular warfare and strategic competition, with a focus on understanding adversary behavior and developing evidence-based approaches to security challenges in contested information environments.

The 2023 operations in the information environment (OIE) strategy acknowledges "challenges and limitations identified in Government Accountability Office reports" on assessment and requires the Department of War (DOW) to "improve tools commanders use to assess effectiveness of operations."[1] The strategy, however, identifies the requirement but provides no operational frameworks for execution. This leaves commanders without methods to evaluate whether messages will achieve intended effects before deployment.

Analysis of iatrogenic influence operations identifies "insufficient feedback mechanisms" as the primary enabling condition where organizations "inadvertently create adverse outcomes" because they cannot evaluate message-audience fit before committing resources.[2] The Camp X-Ray photographs illustrate this problem. Images intended to demonstrate humane treatment became global symbols of cruelty because planners lacked frameworks for anticipating foreign audience interpretations of visual content.[3] Eerhart (2025) identified seven indicators signaling iatrogenic risk, including broad audience targeting without segmentation; false cultural lens imposing creator worldviews on recipients; inconsistent messaging across channels; historical mistrust between sources and audiences; over-simplification of complex issues; dynamic environments rapidly outdating content; and insufficient feedback mechanisms.[4]

These assessment gaps stem from the absence of empirically validated frameworks synthesizing fragmented scholarly insights into operational tools. The problem is not lack of research. Multiple disciplines have produced findings on message effectiveness, yet these insights remain confined within disciplinary boundaries, expressed in theoretical language inaccessible to practitioners, and untested across diverse cultural contexts where information operations occur.

This research addresses the assessment problem through development and validation of the Influence Messaging Impact Model (IM2), an eight-variable model enabling systematic assessment of message resonance across cultural contexts. The model synthesizes theoretical traditions spanning elaboration likelihood models, framing theory, narrative transportation, value alignment research, and cultural schema theory into unified assessment capability.[5] We tested the model through survey research of 6,016 respondents across Japan, the Philippines, South Korea, and Taiwan, demonstrating predictive power while revealing cross-national variation in effectiveness drivers.

IM2 enables dual operational applications. For friendly force operations, strategic communicators can evaluate message variants prior to and during development to identify dimensions requiring enhancement, to optimize messenger selection, and to prevent iatrogenic outcomes through evidence-based refinement. For adversary message analysis, intelligence analysts can systematically score adversary messaging to diagnose resonance factors adversaries emphasize, identify structural weaknesses, assess their likely effectiveness, and develop targeted responses exploiting specific deficiencies.

This article proceeds through four sections. Section II synthesizes fragmented scholarly literature and identifies integration gaps IM2 addresses. Section III presents the eight-variable model with operational definitions. Section IV reports empirical validation findings across four countries. Section V discusses operational implications for offensive and defensive information operations; establishes convergent validity with independently developed iatrogenic indicators; and identifies future research directions.

Fragmented Scholarly Insights and Integration Requirements

Scholarly research on message effectiveness splits across multiple academic disciplines. Each provides valuable insights but uses incompatible terminologies, divergent methods, and minimal cross-disciplinary exchange. This fragmentation hampers practitioners seeking evidence-based guidance on whether friendly messages will resonate or if adversary campaigns contain exploitable weaknesses.

Communication studies center on framing theory, showing how messages guide audience interpretation by emphasizing certain issue dimensions over others.[6] Entman's analysis demonstrates that effective frames define problems, diagnose causes, render moral judgments, and propose remedies.[7] This work generated extensive research on frame competition, resonance, and effects across issue domains. Frames highlighting policy costs produce different audience responses than frames stressing moral dimensions or security threats. Yet, framing literature offers minimal guidance on interaction with other persuasion mechanisms or how culture moderates effectiveness across populations. Framing research examines single-dimension effects in isolation, providing strategic communicators with partial insights disconnected from broader persuasion pathways.

Cultural sociology examines symbolic resonance and value alignment, showing that messages activating familiar schemas bypass cognitive resistance.[8] Social judgment theory reveals how audiences evaluate messages against their attitudinal latitudes, accepting content within acceptable ranges while rejecting discrepant information regardless of argument strength.[9] Messages outside audiences' acceptance latitude trigger boomerang effects where persuasion attempts strengthen contrary attitudes. These dynamics explain why messages resonate differently across populations. Messages emphasizing individual achievement and personal responsibility, for example, resonate in individualist cultural contexts but fail, or backfire, in collectivist societies valuing group harmony and mutual obligation. Cultural sociology rarely converts theoretical findings into operational tools accessible to practitioners. The discipline favors interpretive analysis and thick description over systematic measurement instruments enabling rapid assessment of message-audience fit. Practitioners thus confront fragmented insights across separate literatures with incompatible terminologies. These insights were tested on different populations through divergent methods and lacked explicit guidance on how these factors interact or how their importance varies across cultures. This fragmentation created operational gaps that left organizations exposed to systematic failures.

Additionally, current assessment practices emphasize dissemination metrics over substantive resonance evaluation. Organizations track reach (individuals potentially exposed), impressions (times content is displayed), engagement rates (audience members interacting through likes, shares, and comments), and content sharing patterns across platforms. These metrics fail to measure whether audiences interpret messages as intended or if exposure produces desired effects.[10] Dissemination metrics quantify campaign scales but provide no intelligence on actual effectiveness. High reach, coupled with audience rejection, represents operational failure masked by seemingly positive metrics.

Post-deployment surveys represent current best practice for assessing audience reception beyond dissemination measurement. Organizations conduct surveys after campaign completion to evaluate whether target audiences received messages, interpreted content correctly, and changed attitudes or behaviors. These reactive approaches discover problems only after resource

commitment and potential strategic damage. Organizations learn messages failed or produced backlash through retrospective analysis rather than predictive evaluation during development. For counter-messaging operations, this lag means hostile campaigns achieve substantial penetration before defenders can identify vulnerabilities enabling targeted responses. Current practice operates in perpetual reaction mode, discovering friendly message failures post-deployment and identifying adversary weaknesses only after adversary narratives embed within target populations.

The IM2 addresses these fragmentation, measurement, and integration challenges through three innovations. It synthesizes insights from psychology, communication studies, cultural sociology, and political science into a unified eight-variable model identifying factors that can consistently predict message resonance across contexts. Rather than forcing practitioners to navigate incompatible disciplinary terminologies, IM2 provides operationally accessible variable definitions. These enable intelligence analysts to assess adversary messaging and strategic communicators to develop friendly content through a common framework. Each variable incorporates theoretical insights from multiple disciplines while remaining measurable through straightforward protocols accessible to practitioners without specialized academic training across fields.

The model recognizes that resonance emerges through variable interaction rather than simple additive combination. Individual variables may achieve statistical significance when analyzed separately, but sustained effectiveness requires reinforcement through multiple pathways operating simultaneously. Empirical validation, consistent with the Elaboration Likelihood Model and Heuristic-Systematic Model, showed certain variable combinations produce multiplicative rather than additive effects, with messenger credibility operating as a moderating factor fundamentally amplifying or nullifying content impact.[11] Messages exhibiting strong value alignment and emotional salience but delivered through sources audiences' distrust, for example, face systematic rejection regardless of content quality. Conversely, highly credible sources enhance reception of content that might otherwise face skepticism based purely on substance. This enables practitioners to identify not only the weak individual dimensions but identify how variables combine to amplify or cancel each other's effects.

The model incorporates population-specific calibration through cross-national validation research, demonstrating that universal mechanisms operate with culturally variable weighting across populations. The research revealed which factors matter universally, which vary substantially across countries and require cultural adaptation, and how their relative importance shifts across cultural contexts. Individual value alignment emerged as universally important variable across all examined populations, but effect magnitude varied substantially (more than twice as powerful in South Korea compared to Taiwan). Cognitive engagement mattered significantly in Japan, South Korea, and Taiwan but proved statistically insignificant in the Philippines, suggesting message optimization strategies emphasizing intellectual complexity would succeed in some contexts but fail in others. The IM2's cultural sensitivity enables precise assessment tailored to specific operational environments rather than relying on generic effectiveness criteria assumed universally applicable.

Having identified these disciplinary gaps and integration challenges, we now turn to the IM2 itself, showing how it synthesizes these fragmented insights into a unified operational tool.

The Influence Messaging Impact Model (IM2): Theoretical Foundations and Operational Definitions

The IM2 synthesizes fragmented theoretical traditions into a unified model. The model demonstrates that message resonance emerges through synergistic interactions among eight variables spanning cognitive, affective, and cultural dimensions of human information processing. These variables function not as isolated elements but rather as interacting components of a complex system where their combined presence and mutual reinforcement determine overall resonance potential of messages.

Value Alignment evaluates the semantic and symbolic congruence between message content and audience value systems, including ideological commitments, cultural beliefs, and moral frameworks.[12] This variable captures how effectively messages activate familiar cognitive schemas and fall within audiences' latitude of acceptance, thereby bypassing resistance that would otherwise trigger rejection. Messages exhibiting strong value alignment explicitly reference moral frameworks, cultural narratives, or identity constructs resonating with target audience worldviews. Research distinguishes between Individual Value Alignment (connecting message content to personal priorities such as family security, economic prosperity, or personal achievement) and National Value Alignment (addressing collective concerns about national sovereignty, shared identity, strategic interests, or threats to group wellbeing).[13]

For friendly message assessment, value alignment indicates whether content will resonate with intended audiences by activating existing belief structures rather than requiring fundamental attitude change. A message promoting economic liberalization resonates differently with audiences prioritizing material prosperity versus audiences emphasizing traditional values and social stability. Messages falling outside audiences' latitude of acceptance face systematic rejection regardless of other message characteristics—no amount of emotional salience, narrative coherence, or messenger credibility can compensate for fundamental value misalignment. The empirical validation demonstrated that value alignment operates as the most powerful single predictor across all examined populations, establishing it as the foundational prerequisite for effectiveness. For adversary message analysis, this variable reveals whether adversary messaging successfully connects to target population priorities or exhibits exploitable misalignment. Adversary messages promoting values inconsistent with target audience beliefs create opportunities for counter-messaging systematically emphasizing this disconnect. An adversary campaign emphasizing collective sacrifice might exhibit fundamental misalignment in individualist societies prioritizing personal freedom, creating vulnerability to counter-messaging and thereby highlighting this value disconnect.

Emotional Salience measures messages' capacity to evoke core emotions that drive attention allocation, memory retention, and potential behavioral action. This variable recognizes that emotion functions both as an attention capture mechanism in crowded information environments and as a memory anchor, enhancing long-term retention. High arousal emotions prove particularly effective at enhancing message virality through social transmission and improving recall over time.[14] Messages exhibiting strong emotional salience employ vivid imagery, morally charged terminology, and high arousal emotional frames that evoke visceral reactions such as hope, fear, pride, or anger. Emotional content activates intuitive processing pathways that bypass deliberative scrutiny, thereby reducing counterargument and increasing likelihood of message acceptance through affective rather than cognitive routes.

Cognitive Engagement reflects the mental effort required by messages and the depth of

elaboration they stimulate in the target audience. This variable captures whether messages invite deeper processing through central-route mechanisms that produce durable attitude change or rely on peripheral cues generating temporary compliance without fundamental belief revision.[15] Messages systematically processed through central routes tend to produce more durable attitude change and greater resistance to subsequent counter-messaging compared to messages processed superficially through peripheral routes. The distinction proves operationally significant because attitudes formed through central routes persist longer, resist counter-arguments more effectively, and are more likely to guide subsequent behavior.

Narrative Coherence captures the structural clarity and immersive potential created through storytelling elements including plot development, character identification, and causal attribution. This variable recognizes that audiences more readily internalize messages embedded within compelling narratives that mirror their lived experiences or resonate with familiar cultural contexts.[16] Messages exhibiting strong narrative coherence feature recognizable protagonists and antagonists, clear event sequencing with logical causal connections, and emotionally resonant narrative arcs facilitating psychological immersion. Transportation into narrative worlds reduces counterarguing by engaging audiences emotionally and experientially rather than purely analytically. This enhances persuasion through reduced resistance because transported audiences temporarily suspend critical evaluation while engaging with story content.

Messenger Credibility assesses the perceived trustworthiness, authority, and cultural relevance of message sources within target audiences. This variable recognizes that messenger identity can fundamentally amplify or nullify message impact regardless of content quality. Credible sources who share cultural identity or experiential background with target audiences significantly enhance message uptake and reduce resistance.[17] Messages exhibiting strong messenger credibility either originate from sources that audiences already trust based on accumulated reputation or strategically incorporate diverse voices that broaden perceived neutrality. Source credibility operates through multiple mechanisms including expertise (perceived competence and knowledge), trustworthiness (perceived honesty and lack of ulterior motives), and similarity (perceived shared characteristics with audience).

The empirical validation demonstrated patterns consistent with established dual-process theories – particularly the Elaboration Likelihood Model and Heuristic-Systematic Model – where messenger credibility operates multiplicatively rather than additively, fundamentally modulating content reception in ways demanding separate analytic treatment.[18] These theories established since the 1980s specify that source credibility functions conditionally – as a peripheral cue under low elaboration; as a biasing factor under moderate elaboration; or as irrelevant under high elaboration.[19] Even optimally designed content exhibiting strong value alignment, emotional salience, and narrative coherence faces systematic reception barriers when delivered by sources audiences view as fundamentally untrustworthy. A technically accurate message delivered through a source with history of deception faces rejection based primarily on source characteristics rather than content quality. Conversely, highly credible sources can enhance reception of content that might otherwise face skepticism. For friendly operations, systematic messenger optimization ensures content reaches audiences through sources perceived as trustworthy rather than through sources triggering automatic skepticism. This requires careful analysis of target audience perceptions regarding different potential sources and strategic selection based on their credibility with specific populations. For counter-messaging operations, adversary messages delivered through

sources lacking credibility with target populations reveal structural vulnerability where even substantively strong content faces rejection based primarily on source characteristics.

Symbolic Resonance identifies the deployment of shared symbols, metaphors, and narratives that tap into group identity or activate cultural memory within target audiences. This variable captures how messages draw upon socially constructed meaning systems to structure interpretation and evoke collective responses rooted in shared cultural understanding.[20] Messages exhibiting strong symbolic resonance explicitly invoke cultural motifs, deploy familiar icons or imagery, or reference shared myths and historical narratives carrying pre-established emotional and cognitive associations within particular cultural contexts. Cultural symbols provide interpretive shortcuts enabling audiences to situate messages within familiar frames without requiring extensive cognitive processing of detailed arguments. Symbols compress complex meaning into readily recognizable forms that audiences can process rapidly while activating rich networks of associated meanings, emotions, and memories.

Framing examines the interpretive lenses messages provided by emphasizing certain dimensions while downplaying others, thereby guiding audience attention, and shaping causal attributions along with normative evaluations. This variable captures how messages strategically highlight particular aspects of complex issues—safety concerns, economic impacts, procedural fairness, moral imperatives, etc.—to guide interpretation along preferred dimensions.[21] Effective framing aligns with audience predispositions and existing concerns rather than requiring fundamental belief revision. Frames operate by making certain considerations more salient and accessible when audiences evaluate issues, thereby shaping which criteria they employ when forming judgments and which dimensions receive greater weight in overall assessments.

For friendly operations, strategic framing ensures messages resonate with audiences' existing concerns and values rather than attempting to impose foreign interpretive frameworks. Different frames emphasizing security threats, economic opportunities, procedural fairness, or moral obligations may resonate differently across populations based on their preexisting priorities. In contexts where security concerns dominate public discourse, messages framed in security terms prove more effective than identical content framed in economic terms. For counter-messaging operations, adversary frames misaligned with target audience priorities or emphasizing dimensions audiences view as less salient than other available interpretations create opportunities for systematic reframing that shifts interpretation toward perspectives more favorable to friendly force narratives.

Contextual Fit accounts for temporal appropriateness and situational relevance, considering current events, historical tensions specific to particular audiences, and the broader media ecosystem within which messages circulate. This variable recognizes that messages resonate more strongly when temporally aligned with attention windows and when they leverage situational dynamics making particular frames or claims especially salient at specific moments.[22] Messages exhibiting strong contextual fit coordinate strategically with policy announcements, technical report publications, or other high-attention moments, demonstrating responsiveness to evolving information environments rather than appearing detached from current developments. Contextual fit enables messages to capitalize on existing audience attention and interest rather than requiring creation of entirely new concerns or priorities.

In friendly message timing decisions, ensuring contextual fit maximizes deployment during windows of peak audience receptivity when particular issues already occupy public attention. Messages deployed during these windows

Table 1. Influence Messaging Impact Model (IM2) Variable Definitions

Variable	Definition	Key Characteristics
Individual Value Alignment*	Congruence between message content and audience personal value systems (family security, economic prosperity, personal freedom, health/safety)	Activates familiar cognitive schemas; bypasses resistance mechanisms; explicitly references moral frameworks
National Value Alignment*	Congruence between message content and audience collective values (sovereignty, national pride, strategic interests, collective destiny)	Addresses group-level concerns; invokes national identity; emphasizes collective interests
Emotional Salience	Message ability to evoke core emotions (hope, fear, pride, anger) driving attention and memory retention	Functions as attention-capture mechanism; enhances virality and recall; employs vivid imagery
Cognitive Engagement†	Mental effort required by message and depth of elaboration it stimulates	Invites central-route processing; produces durable attitude change; includes statistics, technical terms
Narrative Coherence	Structural clarity and immersive potential through storytelling elements (plot, characters, causal attribution)	Features recognizable protagonists/antagonists; clear event sequencing; emotionally resonant arcs
Messenger Credibility	Perceived trustworthiness, authority, and relevance of message source	Operates multiplicatively; gates audience engagement; shares cultural/experiential identity with audience
Symbolic Resonance	Use of shared symbols, metaphors, and narratives tapping into group identity or cultural memory	Invokes cultural motifs; deploys familiar icons; references shared myths with pre-established associations
Framing+	Interpretive lens provided by emphasizing certain issue dimensions while downplaying others, guiding audience attention and shaping causal attributions	Aligns with audience predispositions; makes specific considerations more salient; shapes evaluation criteria
Contextual Fit‡	Timing and situational relevance considering current events, historical tensions, and media ecosystem	Coordinates with policy announcements; demonstrates responsiveness; leverages attention windows

Note: *Individual Value Alignment and National Value Alignment represent how the IM2 operationalizes the broader Value Alignment construct, distinguishing between individual-level personal values (family security, economic prosperity, personal freedom, etc.) and collective-level societal values (national sovereignty, collective destiny, strategic interests, etc.). †Cognitive Engagement is operationalized as Thought Provoking for empirical validation. +Framing is operationalized as Issue Salience for empirical validation. ‡Contextual Fit is operationalized as Compelling Given Context for the empirical validation.

Source: Authors.

face lower barriers to attention capture because audiences are already focused on related topics. A message about healthcare reform deployed during active legislative debate on healthcare policy capitalizes on existing audience attention while identical content deployed during periods focused on security crises faces greater competition for attention. Contextual appropriateness, however, extends beyond mere timing to encompass substantive alignment with current situations. Messages contradicted by recent observable developments face systematic credibility challenges regardless of their timing. In adversary message analysis, adversary messaging poorly calibrated to current events or advancing claims contradicted by recent developments reveals vulnerability to counter-messaging emphasizing adversary detachment from on-the-ground realities or demonstrating inability to adapt messaging to rapidly changing circumstances.

The IM2 conceptualizes message resonance as emerging from these variables' combined interaction rather than from any single factor operating in isolation. While individual messages rarely express all variables simultaneously or with uniformly high intensity, those messages incorporating multiple variables demonstrate substantially higher likelihood of achieving resonance with target audiences, particularly when variables are strongly expressed and carefully aligned with both cultural dynamics and temporal contexts. Message resonance emerges from combined interaction among all variables rather than from dominance by any single factor. While certain variables carry greater statistical weight in specific cultural contexts, sustained resonance across diverse audiences requires reinforcement through multiple pathways operating simultaneously. Empirical analyses of the model revealed that variable interactions are synergistic or multiplicative rather than purely additive in their combined effects. Combining high Emotional Salience with strong Narrative Coherence and culturally appropriate Symbolic Resonance, for example, produced amplified effects substantially exceeding simple arithmetic aggregation of individual variable contributions. The model explicitly recognizes that resonance exists on a continuum rather than as a binary outcome, enabling practitioners to diagnose which resonance pathways activate successfully and which remain latent or blocked.

The theoretical framework outlined above requires empirical validation to demonstrate predictive capability across cultural contexts. We now present systematic survey research across four countries in East and Southeast Asia to validate the IM2.

Empirical Validation across Four Cultural Contexts

We validated the IM2 through systematic survey research conducted across four countries in East and Southeast Asia. We employed quota sampling procedures to achieve nationally representative samples balanced across age and gender distribution within Japan, the Philippines, South Korea, and Taiwan. Final sample composition totaled 6,016 respondents, which provided us with the largest dataset for message resonance research within geopolitical context. We selected Japan, the Philippines, South Korea, and Taiwan due to their strategic relevance in the Indo-Pacific theater and the cultural variation across these four states that enabled meaningful cross-national comparison of message resonance dynamics. This selection carries explicit generalizability boundaries that readers should consider when interpreting findings. While we expect the IM2's theoretical architecture and its underlying psychological mechanisms to translate across cultural contexts, the empirically derived variable weights, relative importance rankings, and interaction patterns reported here are population-specific and should

not be assumed applicable to other countries or regions, including other Asian states not examined, without independent validation research. The respondent distribution per country was Japan (n=1,504), Philippines (n=1,503), South Korea (n=1,506), and Taiwan (n=1,503).

The survey instrument employed a 2×2 experimental design administered through Qualtrics to online panel respondents in each country. Respondents were randomly assigned to one of four message versions describing regional security dynamics: a neutral control, an emotional language variant, a cultural symbolism variant, and a combined variant. The dependent variable—overall message resonance—was measured as an ordinal rating on a five-point Likert scale capturing whether the message resonated with the respondent given its content and context. Independent variables comprised ten survey operationalizations of the eight IM2 constructs, with Value Alignment disaggregated into Individual and National dimensions and Framing disaggregated into Security Framing, Identity Framing, and Issue Salience to enable more granular measurement. Respondents rated each dimension on parallel five-point scales. We analyzed these relationships using ordered logit regression, appropriate given the ordinal structure of the dependent variable. Messenger Credibility was excluded from the regression models and instead incorporated through a separate probability adjustment reflecting its empirically demonstrated multiplicative rather than additive effect on content reception.

Ordered logit regression analyses identified which variables significantly predicted message resonance by country examined. All four country specific models demonstrated strong overall fit with pseudo-R-squared values ranging from 0.398 to 0.484, all significant at $p < 0.001$, confirming that the model predicts effectively across culturally distinct populations.[23]

Universal Patterns and Cross-National Variation

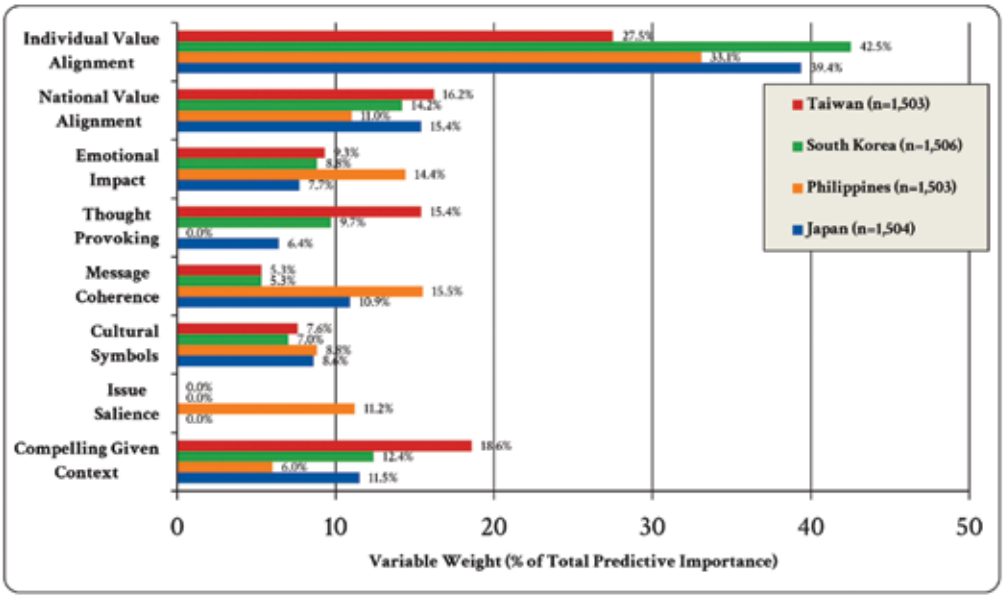
Five variables achieved statistical significance across all four countries without exception: Individual Value Alignment; National Value Alignment; Message Coherence; Contextual Fit (Compelling Given Context); and Emotional Impact. This universal significance pattern suggests core psychological mechanisms that transcend specific cultural boundaries while operating with variable intensity across populations.

Cultural Symbols also proved statistically significant in all contexts, though functioning primarily as supporting element rather than dominant driver. These universally significant factors merit priority attention in both friendly message development and adversary message assessment regardless of specific target population characteristics. (see Figure 1 below)

Individual Value Alignment emerged as the single most powerful predictor across all four countries, though magnitude varied considerably across contexts. South Korea demonstrated the strongest effects, followed by Japan, the Philippines, and Taiwan – with over 1.5-times difference between strongest and weakest effects. Despite this substantial cross-national variation, the universal dominance of individual value alignment underscores that personal value congruence forms the foundation of message resonance regardless of specific cultural context. Messages failing to connect authentically with audience value systems are most likely to face systematic rejection although the severity varies across populations.

Cognitive engagement (Thought Provoking) reached statistical significance in Japan, South Korea, and Taiwan but failed to achieve statistical significance in the Philippines, suggesting differences in cultural values placed on intellectual stimulation and substantive argumentation. The

Figure 1. Variable Weights by Country



Note: Bars represent each variable's percentage contribution to overall message resonance (weights sum to 100% within each country). Zero value indicate variable not statistically significant ($p<0.05$). Variables ordered according to IM2 theoretical model sequence. Data from ordered logit regression analysis.
Total N=6,016; Model fit: pseudo R2=0.398-0.048, all $p<0.001$.

Source: Authors.

Philippines instead showed unique sensitivity to Issue Salience, a pattern not observed in the other three countries. This cross-national variation creates important operational considerations for message optimization. Messages targeting Philippine audiences should prioritize emotional resonance and narrative coherence over purely intellectual complexity, while messages targeting Japan, South Korea, or Taiwan benefit from adequate substantive depth and analytical rigor.

Security Framing and Identity Framing failed to achieve statistical significance across all four countries without exception. Security Framing showed consistently weak effects everywhere, suggesting that threat-based appeals contribute relatively little to overall resonance compared to other available strategies. Identity Framing produced negative coefficients in all four countries though none achieved statistical significance, raising the possibility that explicit identity activation through "us versus them" rhetoric may undermine message effectiveness in these Asian contexts.

Messenger Credibility Effects

The empirical validation revealed that messenger credibility operates differently from content focused variables. Rather than contributing incrementally like other factors, messenger effects amplify or nullify content reception regardless of message quality.[24] Survey research tested this by having respondents evaluate identical message content delivered through sources with varying credibility levels. The pattern proved consistent across all countries: even messages with strong value alignment, emotional impact, and clear narratives faced systematic rejection when delivered through sources distrusted by the intended audiences.

Survey participants indicated which information sources they trusted most, ranked multiple potential messengers, and rated how credibly they

would evaluate identical messages from trusted versus distrusted sources. Analysis revealed substantial credibility differentials between optimal and ill-fitted messengers, with magnitude varying significantly across countries. These differentials reflect how heavily different populations weight source identity when evaluating message validity.

Country specific messenger credibility effects demonstrate meaningful variation in source sensitivity. Japan exhibited the smallest effect at ±8%, indicating Japanese audiences evaluate messages based more on content substance than source identity. The Philippines showed ±14.4% effects, suggesting greater sensitivity to messenger characteristics. South Korea demonstrated the largest effect at ±15.2%, establishing that source selection represents an especially consequential decision when targeting South Korean audiences. Taiwan fell between Japan and the other countries at ±10.2%. These empirical patterns establish that identical content delivered through optimal versus ill-fitted sources could experience effectiveness shifts ranging from 8 percentage points in Japan to more than 15 percentage points in South Korea.

IM2 incorporates these findings through country specific adjustment factors that modify base message resonance scores based on source-audience alignment. Each formula produces no adjustment when messenger credibility is neutral (neither particularly trusted nor distrusted). Optimal messengers, such as universally respected figures, beloved public personalities, or highly credible subject matter experts, generate positive adjustments from +8% to +15.2% depending on country. Conversely, distrusted sources, such as adversary representatives, discredited institutions, or entities known for opposing audience interests, produce negative adjustments of equivalent magnitude. This structure ensures that excellent messages delivered through inappropriate messengers receive proportional penalties while moderate messages delivered through highly credible sources receive appropriate enhancement. (see Figure 2 below)

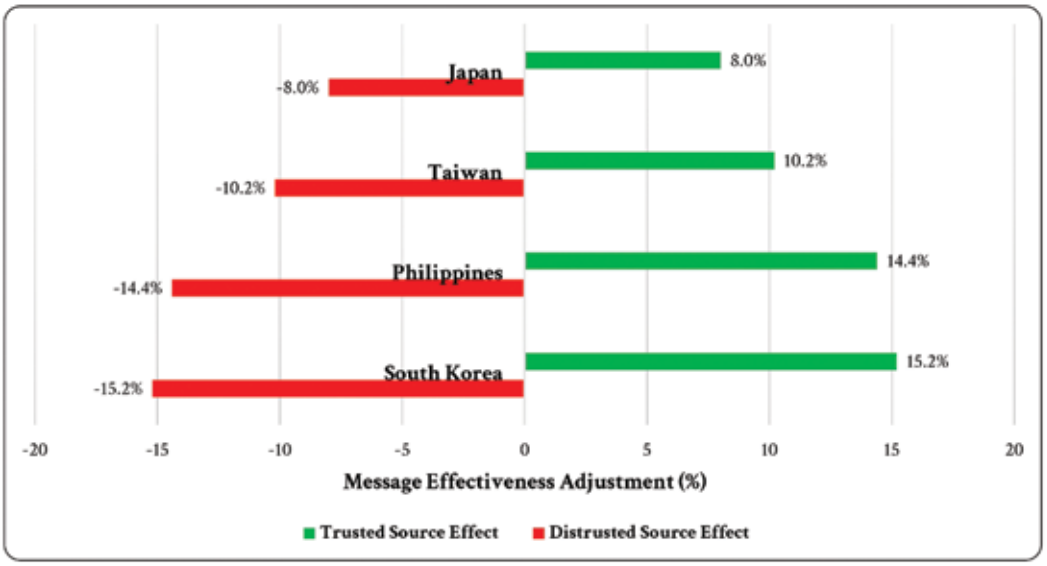
The practical implication is substantial. Source credibility determines whether audiences seriously engage with message content. Messages from distrusted sources face rejection before audiences consider arguments, evidence, or appeals – meaning content optimization cannot compensate for fundamental source-audience misalignment. This explains why organizations sometimes observe systematic message failures despite sound content development, and why identical content achieves dramatically different reception depending solely on who delivered it.

Country Specific Operational Implications

Japanese audiences evaluate messages primarily through the lens of personal value congruence, making individual level alignment absolutely critical for effectiveness. Messages must also exhibit strong contextual fit demonstrating responsiveness to current events and temporal dynamics. Cognitive engagement through intellectually stimulating content matters for Japanese audiences, advising against oversimplification. For adversary assessment, adversary campaigns targeting Japan that emphasize primarily security threats or identity concerns without connecting to individual values should exhibit systematic weakness exploitable through counter-messaging.

Filipino audiences place exceptional premium on narrative clarity and emotional resonance alongside perceived urgency. Messages must tell clear, emotionally compelling stories with logical progression and accessible presentation while framing topics as immediately relevant rather than presenting abstract concerns or distant possibilities. The absence of cognitive engagement effects suggests that intellectual complexity matters less than emotional engagement and narrative clarity. For adversary assessment, adversary messaging in the Philippines exhibiting high cognitive complexity

Figure 2. Messenger Effects Adjustment Range per Country



Note: Bars show percentage adjustment to base message effectiveness score based on messenger credibility. Trusted sources (green) boost effectiveness; distrusted sources (red) reduce effectiveness. A base score of 70 in South Korea could range from 59 (distrusted source) to 81 (trusted source) – a 22-point swing from source selection alone. Data from empirical validation across 6,016 respondents.

Source: Authors.

without corresponding emotional salience may prove systematically less effective than simplified emotional appeals.

South Korean audiences exhibit the strongest value alignment effects observed across all contexts, with individual and national value alignment accounting for a combined 56.7% total explanatory weight. This makes value alignment a fundamental message characteristic necessary to achieve resonance in South Korea. Beyond value alignment, contextual fit proves particularly important. Finally, the exceptionally strong messenger credibility effects in South Korea (±15.2% adjustment range) further underscore the importance of source selection. For friendly operations, careful calibration of both individual and national values combined with strong contextual fit and credible messenger selection are essential. For adversary assessment, exposing value and source misalignments in the message would prove effective in countering adversary campaigns in South Korea.

Taiwanese audiences evaluate messages more holistically than populations in other contexts where individual value alignment dominates overwhelmingly. The relatively balanced contribution across multiple variables suggests that effective messaging in Taiwan requires messages to achieve threshold levels across all significant variables rather than relying on exceptional strength in any single dimension. For adversary assessment, adversary campaigns in Taiwan exhibiting deficiencies across multiple dimensions face compounding vulnerabilities where weaknesses reinforce one another.

Conclusion and Operational Implications

This research program addresses fundamental operational gaps in contemporary information operations. We systematically developed and rigorously validated a framework that enables assessment of message resonance. The IM2 provides

dual-use capability applicable to both offensive and defensive information operations. Organizations can adopt IM2 to evaluate whether friendly messages will achieve intended effects before resource commitment while simultaneously diagnosing exploitable vulnerabilities in adversary campaigns. Beyond its direct operational applications, the IM2's validity receives additional support from an unexpected source – a convergent validation with independently developed indicators of information operations failure.

Convergent Validation with Iatrogenic Indicators

Our prospective theoretical synthesis and empirical testing revealed notable convergence with iatrogenic indicators that Eerhart developed through retrospective analysis of past information campaigns. This convergence through entirely separate analytical pathways validates both frameworks while demonstrating systematic patterns underlying information operations failures. The correspondence demonstrates that IM2 systematically addresses real-world documented failure modes: "Broad General Audience" targeting failures correspond to Value Alignment deficiencies; "False Cultural Lens" vulnerabilities reflect population-specific calibration requirements; "Inconsistent Messaging" manifests as Narrative Coherence deficits; "Historical Mistrust" creates Messenger Credibility challenges; "Over-Simplification" signals insufficient Cognitive Engagement; "Dynamic Environment" failures highlight Contextual Fit assessment gaps; and "Insufficient Feedback Mechanisms" describes precisely the predictive assessment deficit that IM2 addresses.[25] Organizations can prevent these iatrogenic patterns through predictive assessment before deployment while exploiting them in adversary campaigns.

Operational Applications: Friendly Force Message Development

For friendly force operations, the IM2 enables strategic communicators to transform message development from intuition driven art toward evidence-based systematic practice. Practitioners can evaluate multiple message variants during development against population specific effectiveness criteria, optimizing content before deployment. Organizations can conduct iterative assessments throughout development cycles, tracking improvement across successive versions and ensuring final products meet empirically validated effectiveness thresholds before deployment.

The model also enables systematic messenger evaluation based on quantified credibility effects with particular audiences. The empirical validation of established dual-process theory predictions that messenger credibility operates multiplicatively rather than additively, combined with cross-cultural quantification of these effects (±8% to ±15.2%), establishes that source selection represents one of the most consequential decisions affecting overall effectiveness in information operations contexts.[26] Organizations can evaluate multiple potential messengers systematically, assessing their perceived trustworthiness, expertise, and cultural relevance with specific target audiences.

Operationally, organizations should conduct systematic messenger assessments before finalizing campaign plans. This assessment evaluates potential sources across three dimensions: expertise (perceived competence and knowledge), trustworthiness (perceived honesty and lack of ulterior motives), and similarity (perceived shared characteristics with audiences). Messenger selection cannot be treated as an afterthought as it fundamentally determines whether carefully developed content achieves intended effects. Organizations with multiple potential messengers should model expected performance across

alternatives, selecting sources that maximize credibility with specific target populations even when those sources prove less convenient or accessible.

The model's predictive capability enables practitioners to identify messages likely to produce unintended effects before audiences encounter them. By systematically evaluating messages against population specific criteria, organizations can diagnose systematic misalignments between message content and audience value systems, cultural frames inconsistent with target population interpretive schemas, or contextual inappropriateness suggesting likely backlash.

Operational Applications: Adversary Message Analysis and Counter-Messaging

For adversary message analysis, the IM2 enables intelligence analysts to diagnose systematically hostile messaging vulnerabilities and develop targeted operations exploiting identified weaknesses. Intelligence analysts can score adversary messages systematically across eight validated variables to identify empirically which resonance factors hostile actors emphasize most strongly and which dimensions exhibit relative weakness creating exploitation opportunities.

Adversary messaging exhibiting poor value alignment with target populations creates opportunities for counter-messaging systematically emphasizing adversarial actors' fundamental failure to understand target population priorities. Adversary messages lacking coherent narrative structures become vulnerable to counter-messaging, highlighting logical contradictions and emphasizing narrative inconsistencies. Adversary campaigns delivered through sources systematically lacking credibility with target populations enable counter-messaging emphasizing messenger untrustworthiness. Content exhibiting poor contextual fit enables counter-messaging emphasizing adversary detachment from current realities or demonstrating fundamental inability to adapt to changing circumstances.

Messenger credibility patterns can explain why some adversary campaigns fail despite technically competent content development. Adversaries occasionally produce messages exhibiting reasonable value alignment, emotional impact, and narrative coherence but systematically underperform because target audiences reject sources before seriously engaging with content. This pattern appeared frequently in validation data where messages scored highly on content variables but achieved low actual performance when respondents learned source identity. Organizations can predict this pattern through systematic source credibility assessment, enabling forecasts that technically sound adversary content will nonetheless fail when delivered through fundamentally discredited sources.

Operational Efficiency Through Symmetrical Application

The assessment capability operates symmetrically across both friendly message optimization and adversary message exploitation—identical eight variables, consistent scoring protocols, and unified prediction equations apply regardless of application. This fundamental symmetry produces significant operational efficiency gains. Organizations can train personnel on a single integrated model applicable across multiple distinct mission sets. Intelligence analysts developing expertise assessing adversary messaging acquire capabilities directly transferable to friendly message evaluation. The IM2 serves as common operational language spanning offensive and defensive operations. While this research established the IM2's operational utility and empirical validity, several avenues exist for extending the model's capabilities and applicability.

Several alternative explanations warrant acknowledgment. Cultural response styles introduced observable bias in Japan and South Korea,

where respondents exhibited well-documented tendencies to avoid extreme scale positions, concentrating responses within the middle three categories rather than selecting endpoints such as "strongly agree" or "strongly disagree." Despite this compression of response distributions, ordered logit models for both countries still produced statistically significant variation across variables with strong model fit, indicating that the IM2 captured meaningful differences in resonance drivers rather than measurement artifacts. Random assignment to experimental conditions mitigated respondent-level confounds, and the consistent failure of Security Framing and Identity Framing across all four countries despite identical measurement methods suggests that common method variance did not uniformly inflate results. The online panel sampling approach may underrepresent populations with limited digital access, though high internet penetration rates across all four countries partially offset this concern. Finally, the experimental vignettes necessarily simplified real-world information environments, and the data reflect a single point in late 2025, establishing boundary conditions that future longitudinal and multimodal research should address.

Future Research Directions

Several priorities exist for extending the model's operational utility. First, expanding validation to additional populations beyond the four Asian countries examined would establish whether identified patterns generalize to other cultural regions. Validation research in Middle Eastern, African, Latin American, and European contexts would substantially enhance confidence in cross-cultural applicability. Second, developing human-in-the-loop automated assessment capabilities through machine learning integration would enable rapid scoring of large message corpuses supporting operational requirements for assessing adversary campaign evolution in near real-time. Third, examining how resonance factors operate across different media environments—from text-based social media to video content to immersive virtual environments—would enable model's adaptation to emerging platforms. Fourth, longitudinal research examining how message effectiveness changes over time would address questions about temporal persistence of effects and vulnerability to counter-messaging.

Conclusion

The operational imperative emerges clearly from this research. Strategic competition in contemporary information environments demands capabilities extending beyond message production and distribution. Success requires systematic frameworks for evaluating whether friendly messages will achieve intended effects before deployment and identifying adversary message weaknesses enabling exploitation through targeted information operations. The IM2 provides these dual-use capabilities, transforming information operations from reactive assessment toward predictive evaluation preventing failures before resource commitment combined with systematic vulnerability identification enabling proactive exploitation of adversary weaknesses.

Organizations continuing to operate without validated message assessment capability will systematically underperform relative to adversaries employing evidence-based approaches. The IM2 enables movement beyond atheoretical best practices toward evidence-based message development calibrated to specific populations. For defensive operations, it enables systematic adversary assessment identifying exploitable weaknesses enabling targeted counter-messaging rather than reactive generic rebuttals.

Endnotes

[1] U.S. Department of Defense, *Strategy for Operations in the Information Environment* (Washington, DC: Department of Defense, 2023), 8, 13.
[2] Daniel Eerhart. "The Iatrogenic Paradox: When Information Operations Undermine Strategic Objectives," *PRISM* 11, no. 1 (2025): 103.
[3] Eerhart, "The Iatrogenic Paradox," 102.
[4] Eerhart, "The Iatrogenic Paradox," 103-107.
[5] For elaboration likelihood models, see, Richard E. Petty and John T. Cacioppo, "The Elaboration Likelihood Model of Persuasion," In *Advances in Experimental Social Psychology*, vol. 25 (New York: Academic Press, 1986), 123-205. https://doi.org/10.1016/S0065-2601(08)60214-2; For framing theory, see, Robert M. Entman, "Framing: Toward Clarification of a Fractured Paradigm," *Journal of Communication* 43, no. 4 (1993): 51-58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x; For narrative transportation, see, Melanie C. Green and Timothy C. Brock, "The Role of Transportation in the Persuasiveness of Public Narratives," *Journal of Personality and Social Psychology* 79, no. 5 (2000): 701-721. https://doi.org/10.1037/0022-3514.79.5.701; For value alignment research, see, Shalom H. Schwartz, "Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries," in *Advances in Experimental Social Psychology*, vol. 25 (New York: Academic Press, 1992), 1-65. https://doi.org/10.1016/S0065-2601(08)60281-6; For cultural schema theory, see Roy G. D'Andrade, *The Development of Cognitive Anthropology* (Cambridge: Cambridge University Press, 1995).
[6] Dennis Chong and James N. Druckman, "Framing Theory," *Annual Review of Political Science* 10, no. 1 (2007): 103-126. https://doi.org/10.1146/annurev.polisci.10.072805.103054.
[7] Entman, "Framing: Toward Clarification of a Fractured Paradigm."
[8] Marshall A. Taylor, Dustin S. Stoltz, and Terence E. McDonnell, "Binding Significance to Form: Cultural Objects, Neural Binding, and Cultural Change," *Poetics* 73 (2019): 1-16. https://doi.org/10.1016/j.poetic.2019.01.005.
[9] Muzafer Sherif and Carl I. Hovland, *Social Judgment: Assimilation and Contrast Effects in Communication and Attitude Change* (New Haven: Yale University Press, 1961). https://psycnet.apa.org/record/1963-06591-000.
[10] Joshua A. Tucker, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. "Social media, political polarization, and political disinformation: A review of the scientific literature." *Political polarization, and political disinformation: a review of the scientific literature (March 19, 2018)* (2018). https://dx.doi.org/10.2139/ssrn.3144139.
[11] Petty and Cacioppo, "The Elaboration Likelihood Model of Persuasion"; Shelly Chaiken, "The heuristic model of persuasion," In *Social influence*, pp. 3-39. (New York: Psychology Press, [1987] 2014). https://doi.org/10.4324/9781315802121.
[12] Sherif and Hovland, *Social Judgement*; Taylor, Stoltz, and McDonnel, "Binding Significance to Form."
[13] Schwartz, "Overview of the Schwartz Theory."
[14] Jennifer S. Lerner and Dacher Keltner, "Fear, Anger, and Risk," *Journal of Personality and Social Psychology* 81, no. 1 (2001): 146-159; Yaxin Chuai and Jichang Zhao, "Anger Can Make Fake News Viral Online," *Frontiers in Physics*, *10* (2022). https://doi.org/10.3389/fphy.2022.970174.
[15] Richard E. Petty and John T. Cacioppo, *Communication and Persuasion: Central and Peripheral Routes to Attitude Change* (New York: Springer, 1986).
[16] Green and Brock, "The Role of Transportation in the Persuasiveness of Public Narratives"; David A. Snow and Robert D. Benford, "Ideology, Frame Resonance, and Participant Mobilization," *International Social Movement Research* 1 (1988): 197-217.
[17] Alix Whiting, Maik Kecinski, Tongzhe Li, Kent D. Messer, and Julia Parker. "The importance of selecting the right messenger: A framed field experiment on recycled water products." *Ecological Economics* 161 (2019): 1-8. https://doi.org/10.1016/j.ecolecon.2019.03.004.
[18] Petty and Cacioppo, "The Elaboration Likelihood Model of Persuasion;" Chaiken, "The heuristic model of persuasion."
[19] Richard E. Petty, John T. Cacioppo, and Rachel Goldman, "Personal involvement as a determinant of argument-based persuasion." *Journal of personality and social psychology* 41, no. 5 (1981): 847-855. https://doi.org/10.1037/0022-3514.41.5.847.
[20] Herbert Blumer, *Symbolic Interactionism: Perspective and Method* (Berkeley: University of California Press, 1986).
[21] Entman, "Framing"; Chong and Druckman, "Framing Theory."
[22] Snow and Benford, "Ideology, Frame Resonance."

[23] Complete regression output including coefficients, standard errors, and model diagnostics were not included in this article per *PRISM* research article submission guidelines; however, we are happy to provide the complete regression output upon request.
[24] This research confirms theoretical predictions from the Elaboration Likelihood Model and Heuristic-Systematic Model, providing evidence consistent with conditional source credibility effects. Building on Petty, Cacioppo, and Goldman's foundational work from 1981, this research extends our understanding through systematic cross-cultural quantification in the irregular warfare and political communication contexts.
[25] Eerhart, "The Iatrogenic Paradox," 100-113.
[26] Petty and Cacioppo, "The Elaboration Likelihood Model of Persuasion"; Chaiken, "The heuristic model of persuasion."

The Cognitive Domain Is the Main Effort

Why the United States Needs a United States Information Warfare Command

By Dr. Mason M. Moore

Introduction

The United States possesses capable information warfare forces and no organizational architecture to employ them coherently at the national level. Unlike its principal competitors, China, Russia, Iran, and North Korea, the United States lacks a national-level information warfare command. Each adversary has built centralized, nationally directed information warfare structures with pre-delegated execution authorities. The United States distributes its psychological operations, cyber influence, electronic warfare, and military deception capabilities across multiple services and combatant commands with no unifying authority, no coherent national narrative architecture, and an approval process requiring Secretary of War (SECWAR) sign-off before a single message can be transmitted. The Government Accountability Office (GAO) documented this organizational failure in 2021. The 2023 Department of Defense (DoD) Strategy for Operations in the Information Environment (OIE) acknowledged it. Nothing has changed. This article argues for the establishment of a "United States Information Warfare Command" (USIWC): a statutory, joint-interagency, four-star functional combatant command that would close the organizational gap, rationalize authority chains, and restore the United States to credible cognitive competition before the cost of inaction becomes irreversible.

We Are Losing a War Most Americans Do Not Know We Are Fighting

On February 28, 2026, within hours of U.S. airstrikes hitting targets inside Iran, AI-generated videos began flooding global social media. They depicted *Lego*-animated versions of President Trump and Israeli

Dr. Mason M. Moore is a retired U.S. Army Lieutenant Colonel. He previously served as the Department of the Army G-3/5/7's principal Military Information Support Operations integrator and led cognitive effects integration across the department. He holds a Doctorate of Education from Grambling State University.

Prime Minister Netanyahu as panicked figures ordering strikes while Iranian missiles rained down. Rap soundtracks mocked American casualties. *Teletubby*-style caricatures of the President played with toy fighter jets in a miniaturized Oval Office. According to a Clemson University Media Forensics Hub study, dozens of social media accounts affiliated with the Islamic Revolutionary Guard Corps (IRGC) ere operational within 24 hours of the initial U.S.-Israeli strikes, with some content reaching audiences of millions before any coordinated U.S. counter-narrative existed.[1]

Iran's apparatus activated a pre-built playbook. Strategic themes had been established in advance: humiliate American leadership, portray Iran as resilient under attack, frame the conflict as driven by personal scandal rather than national security. Once those themes existed, tactical content producers held standing authority to execute within them without seeking permission for each clip. The *Lego* videos, the rap tracks, and the meme cascades reflect the deliberate output of a pre-authorized, nationally directed cognitive warfare architecture operating at digital speed.[2]

This pattern is not new. On February 24, 2022, the day Russian forces crossed into Ukraine, the Kremlin's information apparatus executed the same playbook. Within hours, coordinated false narratives saturated global social media. By the time Western governments organized a coherent counter-message, the Russian narrative had established itself in the information environment of every country that mattered.[3] Two conflicts, two adversaries, one consistent operational advantage: centralized pre-authorization enabling execution in hours.

Now consider what the United States could have done in response. Under the current architecture, a psychological operations planner at a geographic combatant command (GCC) seeking to counter that narrative would generally need to develop a program, route it through the Joint Staff J39, staff it through the Office of the Assistant Secretary of War for Special Operations and Low-Intensity Conflict (ASW/SOLIC), and obtain appropriate approval before an execute order authorizes execution.[4] While individual steps in that chain can be expedited under time pressure, the structural baseline was not designed to move at digital speed. Individual approvals can be accelerated. The architecture cannot. The result, in a general sense, is a planning and approval cycle measured in days. The adversary moves in hours.

That gap reflects a structural failure of organization, and it is costing the United States dearly.

Multiple authoritative bodies have documented this deficiency over the past decade. The GAO concluded in GAO-21-525T that no single organization leads Department of Defense operations in the information environment.[5] The 2023 DoD Strategy for OIE acknowledged that 'each Service has defined and organized their information forces and capabilities differently' and called for improved integration and deconflicted authorities.[6] That strategy identified the problem in 2023. It is now 2026. The 1st Information Operations Command has been deactivated. The Joint Information Operations Warfare Center has been disestablished. The Army is cutting psychological operations forces to protect its 'shooter' special operators.[7] And China, Russia, Iran, and North Korea are investing more heavily in cognitive warfare than at any point in their history.

Unlike its principal competitors, China, Russia, Iran, and North Korea, the United States lacks a national-level information warfare command. It is time to build one.

This article makes the case for a structural solution: the establishment of a USIWC. The argument is grounded in current joint doctrine, adversary organizational analysis, and the organizational logic that has already produced U.S. Special Operations Command (SOCOM), U.S. Cyber Command (CYBERCOM), and U.S. Space Command

(SPACECOM). It draws on independent research from the *RAND Corporation*, the *Institute for the Study of War* (ISW), and the practitioners who have worked inside the broken system and documented how it fails. The recommendation is concrete, achievable, and overdue.

This article first examines adversary organizational models to establish the structural asymmetry the United States must resolve, then assesses the current U.S. information warfare architecture against the same dimensions and finally proposes a concrete organizational solution and a legislative path to close the gap.

I. The Adversaries Have Already Solved the Problem

Before arguing for what the United States should build, it is worth examining what its adversaries have already built. The organizational analysis is striking not for its complexity but for its consistency: every principal U.S. adversary has independently arrived at the same structural answer.

China: Information Dominance as the Foundation of Everything Else

China's People's Liberation Army (PLA) does not treat information warfare as a supporting function. It treats it as the foundational precondition for achieving dominance in every other domain. The 2013 Academy of Military Science, *Science of Military Strategy,* stated explicitly that "information dominance is the foundation for seizing battlefield initiative; without information dominance it will be difficult to effectively organize friendly forces to seize command of the air and command of the sea."[8] The PLA put its organizational structure where its doctrine is.

The PLA's Strategic Support Force, established in December 2015, consolidates space, cyber, electronic warfare (EW), psychological operations, and technical reconnaissance capabilities under a single theater-level command structure. Open-source estimates place Strategic Support Force personnel between 100,000 and 175,000 across their missions. Strategic Support Force Base 311 in Fujian Province is the dedicated psychological operations unit. The civil-military fusion model multiplies this capacity further, integrating state-owned enterprises, university researchers, and Ministry of State Security contractors into what PLA researchers describe as a 'whole-of-society' information warfare effort.[9]

More revealing than the organizational structure is what PLA researchers say about the United States. A 2019 article by researchers at the PLA National University of Defense Technology, drawing lessons from U.S. psychological warfare, called for China to 'establish a unified leadership and command organization at the national level' for psychological warfare under integrated joint operations, drawing on U.S. organizational models as comparative benchmarks for national-level command integration.[10] China's military is building toward the organization the United States has not yet built, using the United States as its benchmark.

Russia: Cognitive Warfare as a Way of Governance

Russia treats cognitive warfare as a permanent, continuous instrument of governance and geopolitical competition rather than a wartime capability activated in crisis. A June 2025 analysis by ISW documents this comprehensively: cognitive warfare is Russia's way of war, governance, and occupation.[11]

The organizational architecture that sustains this capability is layered and integrated. Authority flows from the Presidential Administration through the Security Council of Russia, coordinating the Main Intelligence Directorate (GRU), the Federal Security Service (FSB), and the Foreign Intelligence Service (SVR) in their respective spheres. State media outlets provide overt narrative dissemination capability. A network of proxy websites,

content-sharing agreements with foreign media, and individual cognitive warfighters, including oligarchs, nationalist commentators, and prominent bloggers deployed as narrative assets, provide human-dimension amplification at scale.[12]

The critical operational characteristic of this architecture is its pre-authorization. Russian information operations do not require individual approval for each action. They operate within pre-approved thematic frameworks, understanding Presidential guidance, enabling tactical actors to execute in hours without seeking permission from senior authorities. That is precisely the model the United States cannot currently replicate.[13]

Iran's information operations following the January 2020 U.S. strike on Qasem Soleimani deployed false imagery and fabricated casualty figures across social media platforms within hours of the event.[14] The United States had no organizational capacity to respond at comparable speed.

Iran and North Korea: Asymmetric Multipliers

Iran maintains its information warfare architecture as a standing national system with pre-delegated authority, enabling execution in hours rather than days. The Supreme Council of Cyberspace, established in 2012 under direct Supreme Leader authority, provides national-level coordination. IRGC Cyber Electronic Command serves as the primary military executor. Iranian operatives maintain a high degree of autonomy once strategic direction is assigned, per the U.S. Army Asymmetric Warfare Group's assessment, making the approval-to-execution cycle extremely short.[15]

The 2026 war with Iran has made that architecture visible in real time. Within hours of U.S. and Israeli strikes February 28, 2026, IRGC's cognitive apparatus activated. The strategic themes were not improvised: humiliate American leadership, portray Iran as resilient under attack, frame the conflict as a distraction from domestic scandal, and depict U.S. military action as cruel and ineffective.[16] Based on observable patterns and open-source reporting, once those themes were established at the national level, tactical producers appear to have had standing authority to execute content within them without seeking permission for each product. The result was a coordinated, AI-generated propaganda campaign that saturated global social media before the United States had produced a single pre-planned counter-narrative.

The content itself demonstrated a level of creative and technical sophistication that surprised Western analysts. *Lego*-animated sequences depicted miniature Trump and Netanyahu figures ordering strikes while Iranian missiles rained down on blocky American warships. AI-generated rap tracks with English-language lyrics targeted American domestic audiences, referencing conspiracy narratives and casting U.S. service members as victims of political cynicism.[17] Videos attributed to the Revayat-e Fath Institute and affiliated accounts were broadcast on Iranian state television and amplified by Iranian embassies in Lebanon, Afghanistan, and South Africa in multiple languages.[18] One video reached more than fifty million views before platform action was taken.

Mapping the Iranian campaign to the authority structure this article proposes is instructive. Open-source assessments and observable patterns indicate that the Supreme Leader and IRGC Qods Force set strategic themes in advance, the equivalent of a Tier 0 information warfare concept. State media and centralized content studios then executed at the national narrative level, the Tier 1 equivalent, pushing standardized content within hours of U.S. moves without seeking new approvals. Iranian embassies, proxy networks, and sympathizer accounts localized and amplified across regional audiences, functioning as the Tier 2 and Tier 3 execution layers. The observable

architecture suggests a standing pre-authorization for tactical and operational activities. No per-product approval chain visible. No program submitted through a joint staff. No execute order awaited.[19]

The United States had no equivalent architecture. The U.S. response to Iran's opening information campaign was uncoordinated, reactive, and inconsistent in its messaging. Academic researchers who analyzed the exchange found that U.S. content lacked message discipline across channels and demonstrated no coherent counter-narrative architecture. A University of Georgia communications professor who studies propaganda assessed the U.S. effort as exhibiting no message discipline and described it as "all over the place."[20] That outcome was not the result of inadequate talent or insufficient effort. It was the predictable output of a government that entered an active cognitive competition without a pre-approved counter-narrative framework, without a command responsible for building one, and without the organizational architecture to execute one in time to matter.

North Korea's Reconnaissance General Bureau directs Bureau 121, a cyber and information warfare unit assessed at approximately 6,000 personnel organized into specialized groups for espionage, financial crime, and high-profile offensive operations.[21] According to UN Panel of Experts assessments, North Korean cyber operations generated over three billion dollars in cryptocurrency theft between 2017 and 2024, funding weapons programs while demonstrating the capacity to penetrate advanced adversary financial systems.[22] The regime also employs strategic deception as a routine instrument: the 2012 missile launch deception, in which North Korea staged a false cancellation before executing the launch on schedule, successfully manipulated the international intelligence community.[23]

The pattern across all four adversaries is unmistakable. Centralized national command authority. Pre-delegated operational powers. Cyber, electronic warfare, and psychological operations integrated under unified direction. Approval timelines measured in hours. Dedicated professional workforces with clear career paths and senior leadership representation. Each adversary arrived at this same organizational solution independently, because it works.

Across these four competitors, the comparison with the United States is stark. Where adversaries possess national-level information warfare commands with pre-delegated authorities and integrated narrative architecture, the United States alone lacks such a command, has no unifying national narrative authority, and cannot respond to cognitive competition at anything approaching adversary speed.

Comparisons to the United States

- Every principal U.S. adversary operates under pre-delegated national information warfare authority, enabling hour-level response. The United States requires days to weeks for the same actions.
- Centralized command structures allow adversaries to integrate cyber, electronic warfare, and psychological operations as a unified capability. The United States addresses each separately, under different commands, without an integrating authority.
- Adversary workforces have clear career paths, dedicated commands, and senior leadership advocates. U.S. information warfare professionals have none of these structural advantages.
- Section II examines what the United States has instead, and why the 2023 DoD strategy, for all its diagnostic clarity, did not produce structural change.

II. What the United States Has Instead: Fragmented Forces, No Command

The United States fields talented, dedicated information warfare professionals across a fragmented organizational structure that systematically prevents them from generating coherent national-level effect. The problem is structural rather than human, and structural problems require structural remedies.

Current State: Fragmented U.S. Information Warfare Enterprise

The current U.S. information warfare architecture comprises the following disparate capabilities, none integrated under a national command authority:

- **Psychological operations (Military Information Support Operations-MISO): Army** forces are organized under U.S. Army Special Operations Command, with the 4th and 8th Psychological Operations Groups at Fort Bragg. This includes 2nd and 7th Psychological Operations Groups (Reserves) organized under the U.S. Army Civil Affairs and Psychological Operations Command. Marine forces are organized under the Marine Corps Information Operations Command.
- **Cyber influence:** Capabilities resident in CYBERCOM and service cyber components, which are oriented primarily toward network operations
- **Electronic warfare:** Assets embedded across all services without a cross-service integration mechanism
- **Military deception and operations security:** Planning functions distributed across joint commands and service staffs
- **Web operations:** The Joint MISO Web Operations Center, under SOCOM in Tampa, Florida
- **Space information operations:** Capabilities under U.S. Space Force Space Delta 10, which are addressed in service doctrine
- **Interagency coordination:** Functions shared with the Department of State's (DoS) Bureau of Global Public Affairs (GPA), but without a Department of War (DoW) integrating authority

Every service employs a different name for the same general concept. The Air Force calls it 'information warfare.' The Army uses 'information advantage activities.' The Marine Corps refers to OIE. The Navy employs the 'information warfare community' construct.[24] The fragmentation reflects the absence of any authority with the mandate to establish common frameworks, common language, and common career paths across the joint information warfare community.

The Approval Problem

Joint Publication 3-13.2, *Military Information Support Operations*, describes the current approval chain for psychological operations programs with precision.[25] Geographic combatant commanders develop proposed programs, which are submitted through the Joint Staff. ASW/SOLIC reviews and staffs the psychological operations portions through the interagency coordination process. SECWAR approves the program as part of the plan. An execute order is then transmitted to the combatant command. All messages and actions for psychological effect must comply with the approved program, and execution authority is delegated to the appropriate level in that execute order.

This process exists for legitimate reasons. It maintains civilian oversight, legal compliance, and interagency coordination in a domain where operational errors carry significant diplomatic and legal consequences. No serious analyst argues for unconstrained execution authority. But the current architecture conflates routine tactical and

operational activities, which should be pre-authorized and executable without individual program review, with strategic-level operations, which appropriately require senior civilian oversight.

Russia, China, and Iran make this distinction cleanly. Their tactical and operational information warfare activities are executed within pre-approved strategic frameworks, reserving senior approval authority for genuine strategic decisions. The United States does not make this distinction. The result is an approval process that treats a counter-narrative social media campaign the same as a covert action finding. Where adversaries act in hours, the United States deliberates in days or even weeks.

The 2026 Iran conflict put that deficit on public display. IRGC-affiliated accounts were posting nationally coordinated AI-generated content within hours of U.S. strikes. The U.S. psychological operations apparatus had no pre-approved counter-narrative framework for an Iran contingency, no standing authority to respond at comparable speed, and no command responsible for ensuring that one existed. The result was that the most capable military force in the world watched a regional adversary shape the global information environment of an active conflict while U.S. information professionals waited for approval chains that were never designed to move at the speed of social media.

The Career Problem

RAND Corporation research on U.S. Air Force information warfare, published in 2024, identified a pathology that applies across the joint force: the community 'lacks a unifying identity,' training is characterized as 'preliminary and rudimentary,' and the career field has 'little representation in the service's senior ranks.'[26] In the U.S. Army, the senior information operations officer functional area caps at the rank of colonel.[27] The Army does not consider information operations officer packets at general officer selection boards.

That ceiling carries strategic consequences. The United States has systematically excluded information warfare professionals from the positions where institutional advocacy, resource prioritization, and strategic direction are determined. The predictable result: information warfare loses the budget argument every cycle in which it competes against kinetic capabilities, because no general officer is in the room to make the case.

The institutional consequences are concrete. Congressional Research Service (CRS) reporting from 2024 documented that Army service leaders were considering cuts to MISO forces specifically to protect 'shooter' special operators. The Army's 2025 *Transformation Initiative* deactivated the 1st Information Operations Command on May 8, 2025, replacing it with Theater Information Advantage Detachments. The Joint Information Operations Warfare Center, a chairman-controlled activity providing joint integration support across the combatant commands, has been disestablished.[28]

The 1st Information Operations Command was deactivated in 2025. The Joint Information Operations Warfare Center was disestablished. The Army is cutting MISO forces. China, Russia, Iran, and North Korea are expanding theirs.

Why the 2023 Strategy for OIE Did Not Fix It

The 2023 DoD strategy for OIE is a competent and honest document. It acknowledges that "each Service has defined and organized their information forces and capabilities differently." It directs improved "integration and oversight of information forces" and calls for action "to develop, update, and deconflict authorities and permissions."[29] In this respect, it is structurally identical to the strategies that preceded it. The same gaps have been identified in successive GAO reports, congressional testimonies, *RAND* studies, and DoD strategy documents for more than a decade without resolution.[30]

The reason those acknowledgments have not produced structural change is simple: the organizations assigned to implement the recommendations lack the authority to do so. The Office of Information Operations and Integration Policy within the Office of the Under Secretary of War for Policy (OSW/P) has policy development authority, strategic oversight responsibility, and interagency coordination relationships. It has no operational command, no dedicated execution capacity, and no authority to task or direct combatant command information operations activities. The Strategic Information Oversight Board established by SECWAR is a deliberative forum, not an operational headquarters.

Working groups and strategy documents can identify problems with precision. Only commands can fix them. The United States has produced more of the former. It needs to build the latter.

Implications: The Gap in Plain Terms

- Where adversaries respond to information environment events in hours under pre-approved authorities, U.S. approval timelines require days to weeks. That is a structural speed deficit, not a talent deficit.
- Where adversaries have national-level narrative coordination authorities integrating cyber, electronic warfare, and psychological operations, the United States has no such integrating authority at any level of command.
- Where adversaries maintain career paths that produce general officers with institutional advocacy for information warfare, the U.S. Army caps its senior information operations officer at colonel, systematically cutting information warfare professionals out of the rooms where resource decisions are made.
- The cumulative result is a nation outcompeted in the domain its adversaries have chosen as their primary axis of effort, not because of inferior talent or technology, but because of inferior organizational architecture. Section III proposes a structural solution.

III. Building a USIWC: The Organizational Answer We Already Know How to Use

The organizational problems documented above do not require new doctrine to solve. Joint Publication 3-0 already elevated information to the seventh joint function in 2018.[31] The DoW's own strategies already identify the gaps with precision. What is missing is the organizational structure to execute. USIWC would be that structure.

The Organizing Logic: We Have Done This Before

The Goldwater-Nichols Act codified a principle in 1986 that remains the theoretical foundation for every unified functional command the United States has since established: fragmented service authorities generate coordination costs, duplicated effort, and weakened institutional advocacy that no interagency working group can overcome.[32] Unity of command resolves those pathologies by concentrating authority, accountability, and resources in a single commander. The United States applied this principle to special operations after the failed Iran rescue mission in 1980, to cyberspace after a decade of disconnected service-led network defense, and to space after decades of multi-service redundancy. Each time, the organizational answer was the same: a statutory functional command with a dedicated four-star, a protected budget line, and unambiguous command authority over the assigned mission. The information warfare domain presents the identical structural problem. The answer is the same.

The proposed USIWC applies organizational

logic the United States has already validated three times. It extends the model that produced SOCOM, CYBERCOM, and SPACECOM into the information warfare domain. Each of those commands addressed a challenge previously managed through fragmented service structures with suboptimal integration, authority friction, and resource competition as predictable results. Each required significant investment in organizational development, doctrine, workforce development, and legal framework construction. Each has demonstrated the strategic value of unified command in its respective domain.

SOCOM was established in 1987 after the Goldwater-Nichols Department of Defense Reorganization Act provided the statutory mechanism to address fragmented special operations capabilities.[33] The result: a functional command with a dedicated four-star commander, a protected budget, joint proponent designation for doctrine and training, and a career pathway that has produced some of the most effective military leaders of the past four decades.

CYBERCOM was established as a sub-unified command in 2009 and elevated to a unified combatant command in 2018. The fiscal year 2025 National Defense Authorization Act (NDAA) required the National Academy of Sciences to evaluate alternative organizational models for cyber forces, and Pentagon leadership endorsed the SOCOM model as the organizational template.[34] The information domain presents an analogous, arguably more mature, structural challenge. The organizational solution should be equally familiar.

PLA researchers drew a parallel conclusion in 2019, calling for China to establish a unified national-level psychological warfare command modeled on the organizational principles of U.S. functional commands.[35] China is building toward the organization the United States should already have. It is time for the United States to build it.

This is not the first time the United States has been forced to reckon with the institutional cost of dismantling a dedicated information organization. The United States Information Agency (USIA), established in 1953 and operational through 1999, sustained strategic communication continuity across twelve administrations and the full arc of Cold War competition.[36] Its 1999 abolition and absorption into DoS eliminated the organizational capacity for sustained, whole-of-government narrative coherence that the agency had maintained for four decades. USIWC is not a re-creation of the USIA. It is a military functional command with operational authorities that agency never held. The institutional lesson, however, is the same: when the United States disbands the command responsible for cognitive competition, it cedes the competition.

USIWC would be established as a unified functional combatant command under Title 10, United States Code (USC), with a four-star commander reporting to SECWAR through the Chairman of the Joint Chiefs of Staff (JCS). As a functional, not geographically bound, command, it would hold the mandate and authorities to synchronize information warfare activities across all GCC areas of responsibility and serve as the national level integrating authority for interagency information operations.

The command's mission: plan, coordinate, synchronize, and when directed, execute the full range of information warfare activities across the whole of government to achieve and sustain information advantage for the United States, deter adversary aggression in the cognitive domain, and support national security objectives across the competition continuum.

The command's decisive advantage would not come from its organizational chart. It would come from its authority architecture. USIWC would employ a tiered pre-delegation framework that gives the United States, for the first time, speed parity with adversaries.[37]

- **Tier 0:** National policy decisions, covert action findings, and National Security Council (NSC)-directed operations; approved at Presidential or SECWAR level
- **Tier 1:** National-level narrative operations, Strategic Information Team deployments, and transregional campaign execution within the approved annual campaign plan; authorized at the USIWC commander level without individual program review
- **Tier 2:** Theater-level psychological operations and operations in the information environment; approved at the geographic combatant command level within the USIWC campaign plan framework
- **Tier 3:** Tactical psychological operations, series and product approval, and direct support to maneuver forces; approved at joint force or component commander level per the execute order

This architecture preserves every element of appropriate civilian oversight. Tier 0 still requires Presidential or SECWAR approval. The legal framework governing Title 10 and Title 50 activities, domestic audience protections, and DoS primacy in public diplomacy would remain fully intact. GCCs retain theater command of their assigned information warfare forces; the USIWC provides global integration, national campaign architecture, and the tiered pre-delegation framework within which GCCs execute. What changes is that routine operational activities no longer require the same approval process as covert action. The distinction between routine influence operations and strategic covert action, a distinction adversaries make cleanly, would finally be reflected in U.S. institutional architecture.

Interagency Integration: Inputs, Outputs, and Boundaries

USIWC would not function as an autonomous military command operating in isolation from the broader national security enterprise. Its effectiveness would depend on structured relationships with the principal departments and agencies whose authorities, intelligence, and diplomatic equities intersect with information warfare. Those relationships are defined by what each entity provides to the command and what the command provides in return, with explicit boundaries governing each lane.

DoS provides diplomatic context, theater public affairs posture, and embassy situational awareness to the command's national campaign planning process. USIWC provides DoS' GPA with coordinated narrative frameworks that public diplomacy activities can amplify without contradicting military messaging. State retains primacy in public diplomacy. At the strategic level, where tensions arise between military messaging and diplomatic signaling, the NSC is the resolution mechanism, not unilateral command action. In the field, a U.S. Ambassador, as Chief of Mission, can utilize his/her designated authorities to adjudicate issues as needed.

The Federal Bureau of Investigation (FBI) and the Department of Justice (DoJ) provide foreign influence indictments, domestic threat assessments, and attribution products for hostile information operations targeting the United States. The command provides military intelligence assessments of foreign cognitive campaigns to inform national security investigations and prosecutions. USIWC holds no domestic authorities. The relationship is limited to outbound intelligence sharing and inbound threat data. That boundary is absolute.

The Central Intelligence Agency (CIA) provides covert action coordination at the Tier 0 level and human intelligence on adversary narrative

intent and command architecture. The command coordinates overt military influence operations to avoid compromising agency activities. This Title 10 and Title 50 deconfliction function currently occurs informally and inconsistently across multiple commands. USIWC would formalize it through a standing coordination mechanism modeled on existing arrangements between CIA and SOCOM.

The National Security Agency (NSA) and CYBERCOM provide signals intelligence on adversary cognitive campaign architecture and technical collection on information operation infrastructure. USIWC uses that intelligence to sequence narrative operations alongside cyber effects so that information and technical operations reinforce rather than contradict each other. The command would hold a formal supported-supporting relationship with CYBERCOM for cyber-enabled influence operations, USIWC owning the cognitive and narrative dimension and CYBERCOM retaining its network-focused mission.

The Office of the Director of National Intelligence (ODNI) provides the *Annual Threat Assessment* and *National Intelligence Estimates* (NIEs) on adversary cognitive operations, forming the baseline for command campaign planning. USIWC feeds operational threat data derived from execution back to the intelligence community through established channels, contributing military-derived insights that all-source assessments otherwise lack. This feedback loop between operational execution and strategic intelligence production is absent from the current fragmented architecture.

Legal Framework and Oversight

USIWC would operate within an established legal framework. Title 10, USC governs overt military operations, including psychological operations directed at foreign audiences. Title 50 governs covert intelligence activities requiring Presidential findings. These authorities are not new. The command concentrates existing Title 10 military information authorities under a single functional commander and formalizes the coordination mechanism between Title 10 activities and Title 50 covert programs. The boundary between them does not change.

The Smith-Mundt Modernization Act of 2012 permits DoS and the U.S. Agency for Global Media (USAGM) to make certain public diplomacy content available to domestic audiences.[38] It does not alter the prohibition on military psychological operations directed at domestic audiences. That prohibition remains intact within USIWC's construct. USIWC's domestic restriction is a deliberate statutory boundary, not an operational limitation, and no element of the command's proposed authority structure encroaches on it.

In armed conflict, USIWC operations would be conducted consistent with the law of armed conflict. The principles of distinction, proportionality, and precaution apply to information operations as they apply to all military operations.[39] Legal review would proceed through the same processes applicable to every combatant command, with command judge advocates embedded at the headquarters and Strategic Information Team levels.

Congressional oversight would be comprehensive. The USIWC commander would appear before the Senate and House Armed Services Committees for budget and readiness testimony. Programs with covert action or intelligence equities would be subject to applicable intelligence committee review. The DoW Inspector General's (IG) jurisdiction would extend to command activities. Concentrating information warfare authority in a statutory command produces more oversight than the current fragmented architecture, which allows no single committee to exercise complete oversight of the national information warfare enterprise precisely because no such enterprise exists in unified form.

The Strategic Information Teams: Operational Teeth

USIWC would not be solely a headquarters planning and coordination entity. It would maintain organic operational capabilities in standing, cross-functional Strategic Information Teams.[40] Each team is designed to identify, assess, and respond to strategic-level information threats faster than the current approval process permits.

Each Strategic Information Team would comprise specialists across all-source intelligence analysis with behavioral influences training, offensive and defensive cyber operations, electronic warfare and electromagnetic spectrum operations, psychological operations with regional language capability, space information operations, Special Technical Operations, and Civil Affairs. Teams would be regionally aligned with GCCs and with a global response team at USIWC headquarters for transregional surge employment.[41]

Strategic Information Teams would hold Tier 1 pre-delegated authorities, enabling execution of approved response activities within established thematic and legal frameworks without individual approval for each action. The standing instruction is to act within authority rather than wait for approval. That pre-authorization is how the United States finally matches the operational tempo adversaries have enjoyed for years.

Joint Proponent: The Institutional Foundation

USIWC would assume joint proponent authority for psychological operations and information warfare, currently held by SOCOM under Joint Publication 3-13.2.[42] This transfer preserves SOCOM's operational role. The proponent function, which encompasses doctrinal development, program of instruction authority, joint training standards, and career field advocacy, requires a command whose primary institutional identity is information warfare rather than special operations.

Individual service schools would retain their curricula. USIWC's J7 would exercise curriculum approval authority over all courses addressing influence operations, psychological operations, and operations in the information environment across the joint force. USIWC's commander and principal staff would serve as executive lecturers at the National Defense University, creating a permanent pipeline to the next generation of senior national security leaders.

Above all, USIWC would provide the one institutional condition information warfare professionals have never had: a four-star commander in the room where resource decisions are made, equipped with the statutory mandate, the institutional authority, and the career incentives to advocate for the information warfare budget every year.

National Security Council Integration: Positioning the Commander

The National Security Act of 1947 establishes the JCS Chairman as the principal military advisor to the President, the Secretary of Defense, and the NSC. Combatant commanders do not hold seats on the NSC as principals. That statutory boundary does not change with the establishment of the USIWC. This section describes how the USIWC commander's position should be structured relative to the NSC upon the command's establishment.

The White House recently created a NSC staff position titled "Director of Cognitive Advantage." Public descriptions identify this role as part of the NSC staff but do not list it as a voting member of the NSC or the Principal's Committee (PC) and it is most likely organized into the Interagency Policy Committee (IPC) process. These sources describe IPCs as assistant secretary level interagency bodies, often chaired by NSC staff, which inform recommendations reviewed at the Deputies Committee (DC) and PC levels.[43] This potentially places both the

Director of Cognitive Advantage and the USIWC commander at the same functional tier of the NSC system. Upon establishment, the USIWC commander would serve as a standing advisory member of the IPC chaired by the Director of Cognitive Advantage. That is the appropriate and realistic level of access. The USIWC commander is neither a voting principal nor a DC member by default. Rather, the commander's role at the IPC is advisory: providing operational feasibility assessments, campaign planning inputs, and capability data that inform the Director of Cognitive Advantage's policy recommendations as they move upward through the DC and PC tiers.

When the Director of Cognitive Advantage's portfolio generates agenda items that reach the DC, the USIWC commander may be called to brief in a supporting capacity. The USIWC commander does not attend the DC independently. The JCS Chairman carries military equities at that level. Access to the NSC therefore runs through two distinct lanes: through the Director of Cognitive Advantage at the IPC level, and through the Chairman at the DC and PC levels. Those lanes are complementary and should remain structurally separate. Maintaining that distinction preserves both civilian oversight and the institutional integrity of the Chairman's role as the nation's principal military advisor.

What Changes Under USIWC

- **Response timelines:** Tier 1 pre-delegated authorities reduce information operations response from days to hours, closing the adversary speed advantage documented throughout this article.
- **Narrative coherence:** A single national campaign plan, approved annually, replaces eight separate GCC program submissions reviewed sequentially by SECWAR.
- **Career equity:** A four-star command with a joint proponent designation creates the career pathway to general officer rank that information warfare professionals currently lack.
- **Doctrinal unity:** A single joint proponent authority (USIWC J7) reconciles Air Force, Army, Marine Corps, and Navy information warfare frameworks into a common operational concept.

IV. Addressing the Objections

Every significant organizational reform generates objections. Four are predictable and worth addressing directly.

"We Cannot Compete in the Information Domain Because We Are a Democracy"

This objection is factually wrong. Israel, the United Kingdom, and other allied democracies have developed national-level information operations capabilities that demonstrate the compatibility of effective cognitive competition with democratic governance and rule of law. These nations operate under established parliamentary oversight, statutory authorities, and legal constraints governing their information operations, demonstrating that democratic accountability and operational effectiveness reinforce one another rather than conflict.

The United Kingdom's 77th Brigade, established in 2015 as a dedicated information operations formation, provides the most direct allied precedent.[44] The Brigade operates under parliamentary oversight and within British law governing military information activities. Its establishment did not require the United Kingdom to resolve a fundamental incompatibility between democracy and information warfare. It required political will to treat the domain with the institutional seriousness it demands. The United States has demonstrated equivalent political will in standing up SOCOM,

CYBERCOM, and SPACECOM. The information warfare domain warrants the same decision.

The objection also conflates two legally distinct activities: targeting domestic audiences, which Title 10, USC clearly prohibits for psychological operations forces, with competing in the global information environment, which is both legal and strategically essential. USIWC would operate entirely within the existing legal framework: Title 10 and Title 50 boundaries preserved, domestic audience protections intact, DoS primacy in public diplomacy maintained. Democratic oversight would be enhanced, not circumvented, by concentrating information warfare authority in a statutory command subject to the full suite of congressional oversight, IG review, and civilian policy control that applies to every other functional combatant command.

"This Creates Dangerous New Authorities"

USIWC creates no new authorities that do not currently exist. The authorities for psychological operations, cyber influence activities, military deception, and electronic warfare already exist, distributed across the joint force without coherent integration. USIWC consolidates and rationalizes those existing authorities within a single command structure. The pre-delegation framework reduces bureaucratic delays for routine activities while fully maintaining the oversight architecture for sensitive and strategic operations.

Tier 0 national policy approval remains. Covert action still requires a Presidential finding. The significant change is that a counter-narrative social media campaign within an approved thematic framework no longer requires the same approval process as a covert action finding. That change constitutes a rational allocation of existing authority to the appropriate decision level. SOCOM precedent applies directly: tiered authorities rationalized special operations in 1987; the same approach works here.

The Smith-Mundt Modernization Act of 2012 clarified the evolving legal landscape for information activities by permitting certain DoS and public media content to be made available domestically.[45] That statute does not expand military authorities. USIWC's operational boundary at the domestic audience line is grounded in Title 10, not policy preference, and no element of the proposed authority structure crosses it. In armed conflict, operations would proceed under the law of armed conflict, with the same legal review chain that governs every combatant command.[46] The command would not create a legal gray zone. It would concentrate existing authorities in a single commander accountable to the same statutory oversight framework as SOCOM and CYBERCOM.

"We Already Have U.S. Cyber Command"

CYBERCOM is a cyberspace operations command, not an information warfare command. Its authorities, workforce, and operational concept are oriented toward the technical and offensive-defensive dimensions of cyberspace: network operations, cyber-attacks, and cyber defense. Psychological operations, military deception, electronic warfare in the influence dimension, and cognitive warfare are outside CYBERCOM's mission and authorities.

USIWC would complement CYBERCOM's technical domain operations. Cyber-enabled influence operations would be coordinated between the two commands, with USIWC owning the cognitive and narrative dimension and CYBERCOM retaining its network-focused mission. GCCs retain theater command of assigned information warfare forces USIWC provides global integration and campaign architecture within which GCCs execute. These are distinct but interconnected capabilities. Having one does not substitute for the other.

"A New Four-Star Command Is Too Expensive and Too Slow to Build"

USIWC is best understood as a low-regret organizational decision: it primarily reorganizes and integrates existing forces, billets, and facilities rather than creating new capabilities from scratch. The headquarters element of approximately 800 personnel would be drawn from billets that already exist across the joint force and are currently under-integrated. The recommended primary location is the Mark Center campus in Alexandria, Virginia, a DoW-owned facility with 1.8 million square feet of secure office space operated by Washington Headquarters Services (WHS) with significant existing secure office capacity and ongoing space optimization efforts.[47] No new construction is required.

The organizational precedents of SOCOM and CYBERCOM suggest that initial operating capability within 24 months of congressional authorization is achievable. SOCOM stood up in 18 months. CYBERCOM elevated from sub-unified to unified combatant command in less than a year following legislative direction.

The cost argument also runs decisively in the opposite direction. The United States currently spends billions annually on information warfare-related capabilities that cannot achieve coherent national-level effect because no organizational authority exists to synchronize them.[48] The cost of inaction is compounding annually: lost influence in partner nations, eroded alliance cohesion, and adversary information operations that have successfully reshaped strategic relationships. Russian information operations preceding the July 2023 military coup in Niger, which resulted in the expulsion of U.S. and French forces from Air Base 201 at Agadez and other installations, illustrate what persistent, nationally directed cognitive competition produces when one side fields a command and the other relies on a working group.[49]

V. What Action Looks Like

The case for USIWC does not require senior leadership to accept every element of a specific organizational design. It requires acceptance of one foundational proposition: the United States needs a national-level, statutory information warfare command, and the time to build it is now.

The Legislative Vehicle

The mechanism for that decision is the NDAA. Section 161 of Title 10, USC establishes the list of unified combatant commands and requires amendment to add an information warfare command to that list. Congress has used the NDAA before to establish or elevate specialized commands: SOCOM's statutory mandate came from Pub. L. 99-661 (1986); CYBERCOM's elevation to a unified combatant command was directed by Congress in the fiscal year 2017 NDAA; SPACECOM was re-established through the fiscal year 2020 NDAA. A parallel amendment to 10 USC Section 161 to add USIWC as a unified functional combatant command would follow this well-established pattern rather than creating a novel legislative mechanism.

The fiscal year 2025 NDAA directed a study of alternative organizational models for cyber forces.[50] A parallel provision directing the establishment of a USIWC, with a timeline and authorities framework to be developed by the Office of the Secretary of Defense in coordination with the Joint Staff and NSC, is the next logical step in that same policy trajectory.

The Execution Sequence

Congressional action would be the catalyst; executive branch implementation would follow a clear sequence. A joint OSW-Joint Staff planning team, co-chaired by OSW/P and the Vice Chairman of the JCS, would develop the initial

operating capability concept and the pre-delegation authority framework. NSC would develop the Presidential directive establishing USIWC commander's NSC participation and the governance framework for Tier 0 authorities. An interim three-star commander, designated within 90 days of congressional authorization, would begin headquarters activation and initiate the Mark Center facility assessment.

A near-term timeline is achievable. The United States stood up SOCOM in 18 months. It elevated CYBERCOM from sub-unified to unified combatant command in less than a year following legislative direction. The organizational infrastructure, the doctrine, the trained personnel, and the available facilities already exist. What has been missing is the statutory mandate and the four-star commander. The time for study is over. The organizational answer is clear, and delay preserves an approval architecture that ensures U.S. responses remain days behind adversary operations.

Congressional action is the trigger. Not another strategy. Not another working group. Not another DoW study. The NDAA is the vehicle. The time is now.

What Congress Can Do Now

- **Amend 10 USC Section 161** to add a USIWC as a unified functional combatant command, following the same statutory pattern used for SOCOM, CYBERCOM, and SPACECOM.
- **Direct DoW to submit an implementation plan** and tiered authority framework for USIWC within 180 days of enactment, including command relationships with GCCs, CYBERCOM, and SOCOM.
- **Require an annual report** on information warfare readiness and USIWC progress, to include an assessment of adversary information warfare activities and the integration of USIWC capabilities with GCC operations.
- **Authorize pilot Strategic Information Teams** aligned to select theaters in Phase I to demonstrate operational value before full command stand-up, providing a low-cost proof of concept tied to clear milestones.
- **Protect MISO force structure** by including language in the NDAA that identifies psychological operations forces as a congressional interest item and requiring DoW certification before any further reductions to MISO force structure pending USIWC establishment.

Each action stands on its own and can be advanced independently. Together they constitute a coherent legislative agenda, one that would produce the most significant structural improvement to U.S. information warfare since Joint Publication 3-0 elevated information to a joint function in 2018.

Conclusion: The Ground Is Already Occupied

The 2026 war with Iran is the first major conflict in which cognitive competition has been openly waged in real time, on public platforms, with AI-generated content, at industrial speed. Iran activated a nationally coordinated influence campaign within hours of the first U.S. strikes. The United States improvised. The scale was not trivial: available open-source analysis suggests Iranian content achieved attention metrics on par with major U.S. government accounts on the same platforms, and Iran's messaging penetrated not just foreign populations but American domestic audiences, exploiting U.S. political vulnerabilities with a sophistication that no ad hoc public affairs response could match.[51]

The Iran case reflects a recurring pattern. Russian cognitive operations were a significant factor in shaping political elites and public opinion

in Niger, contributing to conditions that enabled the July 2023 coup and the subsequent expulsion of U.S. forces from Air Base 201 at Agadez and other installations. Russia had spent years shaping the information environment of a strategically important country before U.S. forces ever arrived. The same playbook is active in Mali, Burkina Faso, the Central African Republic (CAR), and across the Global South.[52] Russia does not need to match U.S. conventional military power. It needs to shape the information environment of countries where U.S. presence depends on host nation consent. In Iran, in Niger, across the competition continuum: adversaries have a command, and the United States has a working group.

China is running a more sophisticated version of the same operation at global scale. The PLA's cognitive domain operations, which ODNI described in both the 2022 and 2024 *Annual Threat Assessments* as combining psychological warfare with cyber operations to shape adversary behavior and decision-making, are operational, continuous, and directed by a command of more than 100,000 personnel with pre-delegated national-level authority.[53]

The United States has spent twenty-five years and trillions of dollars optimizing its military for the kinetic defeat of adversaries in physical domains. It has neglected, by organizational design rather than deliberate choice, the domain in which its most consequential adversaries have chosen to compete. The cognitive domain is the main effort of 21st-century great power competition. The organizational architecture of the United States does not yet reflect that reality.

Establishing USIWC will not solve every problem in the information environment. It will not automatically counter every Russian narrative or Chinese information operation. What it will do is give the United States, for the first time, a national-level command with the authority, the resources, the pre-delegated operational powers, and the institutional mandate to compete in the cognitive domain persistently, proactively, and at the pace adversaries have long exploited.

USIWC is a low-regret decision. It reorganizes existing forces, uses existing facilities, and follows an organizational template the United States has successfully executed three times in the past four decades. The strategic cost of inaction, however, is not low regret. It compounds every year the United States leaves the cognitive domain to adversaries who have already chosen it as their primary axis of effort.

Congress should authorize USIWC in the next NDAA. SECWAR should stand it up within 24 months. The next generation of national security leaders should inherit a United States that takes the cognitive domain as seriously as its adversaries do.

The U.S.' adversaries have made their organizational decisions. The United States needs to do the same.

Endnotes

[1] Linvill, Darren and Patrick Warren, Media Forensics Hub, Clemson University, cited in "Iran Targets US Public Opinion with Online Information War," *France 24*, March 25, 2026.
[2] Carrie Kahn, "Iran's War Propaganda Includes Memes Directed at Trump," *NPR*, March 26, 2026; "Iran's War Propaganda Hones in on Trump with Lego Memes," *CNBC*, April 1, 2026; "When Virality Is the Message: The New Age of AI Propaganda," *Time*, April 2, 2026.
[3] Nataliya Bugayova and Kateryna Stepanenko, *A Primer on Russian Cognitive Warfare* (Washington, DC: Institute for the Study of War, June 30, 2025).
[4] *Joint Publication 3-13.2, Military Information Support Operations* (Washington, DC: Joint Chiefs of Staff, 2014), chap. III.
[5] Government Accountability Office (GAO), "Information Environment: DoD Operations Need Enhanced Leadership and Integration of Capabilities," GAO-21-525T (Washington, DC: GAO, April 30, 2021); Joseph W. Kirschbaum, Testimony before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, House Committee on Armed Services.
[6] *2023 Department of Defense Strategy for Operations in the Information Environment* (Washington, DC: Office of the Secretary of Defense, July 5, 2023).
[7] Department of the Army, *Army Transformation Initiative* (Washington, DC: Headquarters, Department of the Army, 2025); Congressional Research Service, "U.S. Special Operations Forces: Background and Considerations for Congress" (Washington, DC: CRS, 2025).
[8] People's Liberation Army (PLA), Academy of Military Science, *Science of Military Strategy* (Beijing: Military Science Press, 2013), 130, cited in Beauchamp-Mustafaga, RAND RR-A853-1.
[9] Nathan Beauchamp-Mustafaga, "Chinese Next-Generation Psychological Warfare," *RAND* RR-A853-1 (Santa Monica, CA: RAND Corporation, 2023), 18–22.
[10] Beauchamp-Mustafaga, *RAND* RR-A853-1. The characterization of U.S. organizational models as comparative benchmarks reflects RAND's analysis of primary Chinese-language sources.
[11] Bugayova and Stepanenko, *A Primer on Russian Cognitive Warfare*, 4–9.
[12] Bugayova and Stepanenko, *A Primer on Russian Cognitive Warfare*, 10–16.
[13] Bugayova and Stepanenko, *A Primer on Russian Cognitive Warfare*, 12–14.
[14] U.S. Army Asymmetric Warfare Group, "Iran Quick Reference Guide" (Unclassified, Distribution Statement A, circa 2019).
[15] U.S. Army Asymmetric Warfare Group, "Iran Quick Reference Guide."
[16] Kahn, "Iran's War Propaganda Includes Memes Directed at Trump."
[17] "Iran's War Propaganda Hones In on Trump with Lego Memes," *CNBC*, April 1, 2026.
[18] "When Virality Is the Message: The New Age of AI Propaganda," *Time,* April 2, 2026.
[19] Roger Stahl (University of Georgia), cited in "Iran's War Propaganda Hones in on Trump with Lego Memes," *CNBC*, April 1, 2026; "White House's 'Banger Memes' Trivialize Iran War," *Washington Times*, March 23, 2026. The tiered-authority mapping is the author's analytical framework applied to observable open-source patterns.
[20] Kahn, "Iran's War Propaganda Includes Memes Directed at Trump."
[21] Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: ODNI, February 5, 2024), 10; United Nations Security Council, Panel of Experts on North Korea, S/2024/215 (New York: United Nations, March 2024).
[22] United Nations Panel of Experts on North Korea, annual reports, 2018–2024 (S/2019/171 through S/2024/215).
[23] "North Korea Launches Rocket Despite Warnings," *Associated Press*, December 12, 2012; ODNI, *Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC: ODNI, 2013), 8–11.
[24] Air Force Doctrine Publication 3-13, *Information Operations* (Department of the Air Force, 2023); Army Doctrine Publication 3-13, *Information Operations* (Headquarters, Department of the Army, 2023); Marine Corps Warfighting Publication 3-32, *Marine Air-Ground Task Force Information Operations* (Headquarters, Marine Corps, 2015); OPNAVINST 3430.26D, *Implementation of Information Operations* (Department of the Navy, 2012).
[25] Joint Publication 3-13.2, *Military Information Support Operations* (Washington, DC: Joint Chiefs of Staff, 2014), III-1–III-12.
[26] Alyssa Demus et al., "Operationalizing U.S. Air Force Information Warfare," RRA1740-1 (Santa Monica, CA: RAND Corporation, 2024), xii–xiii.
[27] Army Regulation 614-100, *Officer Assignment Policies, Details, and Transfers*; see also Demus et al., RRA1740-1, xvii.
[28] Congressional Research Service (CRS), "U.S. Special Operations Forces: Background and Considerations for Congress" (Washington, DC: CRS, 2025); Department of the Army, *Army Transformation Initiative* (Washington, DC: Headquarters, Department of the Army, 2025).

[29] 2023 DoD Strategy for OIE, 4–6.
[30] See, e.g., GAO-16-219 (2016); GAO-23-105442 (2023); Demus et al., RRA1740-1 (2024); Beauchamp-Mustafaga, RR-A853-1 (2023).
[31] Joint Publication 3-0, *Joint Operations* (Washington, DC: Joint Chiefs of Staff, incorporating change 1, October 22, 2018), V-13–V-14.
[32] Pub. L. 99-433, *Goldwater-Nichols Department of Defense Reorganization Act of 1986*, 100 Stat. 992 (1986); Pub. L. 99-661, *National Defense Authorization Act for Fiscal Year 1987*, 100 Stat. 3816 (1986) (Cohen-Nunn Amendment establishing U.S. Special Operations Command).
[34] *National Defense Authorization Act for Fiscal Year 2025*, Pub. L. 118-159 (2024); "Pentagon Backs SOCOM Model for Cyber Command amid Calls for Separate Cyber Force," *Federal News Network*, May 20, 2025.
[35] Beauchamp-Mustafaga, RAND RR-A853-1, citing PLA National University of Defense Technology research (2019).
[36] USIA was established by *Reorganization Plan No. 8* of 1953 and operated from August 1, 1953, through October 1, 1999. Its missions were transferred to the Department of State under the *Foreign Affairs Reform and Restructuring Act of 1998*, Pub. L. 105-277. For assessments of the institutional consequences of USIA's abolition, see Nicholas J. Cull, *The Decline and Fall of the United States Information Agency: American Public Diplomacy, 1989–2001* (New York: Palgrave Macmillan, 2012).
[37] The tiered pre-delegation framework is the author's proposed construct, drawn from authority structures in Pub. L. 99-661 (Goldwater Nichols Act) and Joint Publication 3-13.2.
[38] *Smith-Mundt Modernization Act of 2012*, *National Defense Authorization Act for Fiscal Year 2013*, Pub. L. 112-239, § 1078 (2013). The amendment permits the DoS and USAGM to make certain public diplomacy content available domestically. It does not alter 10 U.S.C. § 331 et seq. or the prohibition on military psychological operations directed at domestic audiences.
[39] Department of Defense, *Law of War Manual* (Washington, DC: Office of General Counsel, DoD, June 2015, updated December 2016), §§ 16.1–16.5, addressing information operations, military deception, and psychological operations in the context of the law of armed conflict, including the principles of distinction, proportionality, and precaution.
[40] The Strategic Information Teams concept is the author's original organizational proposal. No equivalent standing, nationally pre-authorized cross-functional information warfare response capability currently exists in U.S. force structure.
[41] Special Technical Operations refers to sensitive activities requiring compartmented planning and execution. See Joint Publication 3-13, *Information Operations* (Washington, DC: Joint Chiefs of Staff, 2014), I-6–I-9.
[42] Joint Publication 3-13.2, *Military Information Support Operations* (Washington, DC: Joint Chiefs of Staff, 2014), chap. III.
[43] United States. Office of the President. "DCPD-202500151 – National Security Presidential Memorandum on Organization of the National Security Council and Subcommittees." Daily Compilation of Presidential Documents. Washington, DC: Office of the Federal Register, National Archives and Records Administration, 2025. Belfer Center for Science and International Affairs. "Explainer: The U.S. National Security Council (NSC)." Harvard Kennedy School, April 6, 2025. The Cipher Brief. "The Country's First 'Cognitive Advantage' Chief: Influence Is the New Battlefield." January 15, 2026
[44] The British Army's 77th Brigade was established in 2015 as a dedicated information operations formation. It operates under the authority of the United Kingdom's Joint Doctrine Publication 3-00 and applicable parliamentary oversight frameworks governing military information activities. See also U.K. Ministry of Defence, *Integrated Review Refresh 2023: Responding to a More Contested and Volatile World* (London: HM Government, 2023).
[45] *Smith-Mundt Modernization Act of 2012*, *National Defense Authorization Act for Fiscal Year 2013*, Pub. L. 112-239, § 1078 (2013). The amendment permits the Department of State and the U.S. Agency for Global Media (USAGM) to make certain public diplomacy content available domestically. It does not alter 10 U.S.C. § 331 et seq. or the prohibition on military psychological operations directed at domestic audiences.
[46] Department of Defense, *Law of War Manual* (Washington, DC: Office of General Counsel, Department of Defense, June 2015, updated December 2016), §§ 16.1--16.5, addressing information operations, military deception, and psychological operations in the context of the law of armed conflict, including the principles of distinction, proportionality, and precaution.
[47] WHS, *Fiscal Year 2025 Budget Estimates, Operation and Maintenance* (Arlington, VA: WHS, March 2024). The Mark Center campus at 4800 Mark Center Drive, Alexandria, Virginia, is a 1.8 million square foot DoW facility operated by WHS with existing secure office capacity supporting multiple defense agencies.
[48] GAO-16-219 (2016), 8–10; GAO-21-525T (2021), 5–7; DoD Comptroller, *Defense Budget Overview, Fiscal Year 2025 President's Budget* (Washington, DC: Office of the Under Secretary of Defense (Comptroller), March 2024).

[49] Bugayova and Stepanenko, *A Primer on Russian Cognitive Warfare*, 17–22; RAND Corporation, "Russia's Use of Influence Operatives in Sub-Saharan Africa" (Santa Monica, CA: RAND Corporation, 2024); Institute for the Study of War (ISW), situational reports on Niger, July–August 2023.
[50] *National Defense Authorization Act for Fiscal Year 2025*, Pub. L. 118-159 (2024); "Pentagon Backs SOCOM Model for Cyber Command amid Calls for Separate Cyber Force," *Federal News Network*, May 20, 2025.
[51] Roger Stahl (University of Georgia), cited in "Iran's War Propaganda Homes In on Trump with Lego Memes," *CNBC*, April 1, 2026; "White House's 'Banger Memes' Trivialize Iran War," *Washington Times*, March 23, 2026.
[52] Bugayova and Stepanenko, *A Primer on Russian Cognitive Warfare*, 17--22; Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: ODNI, February 5, 2024), 16--18 (discussing Russian influence operations in Niger, Mali, and Burkina Faso); Government Accountability Office (GAO), *Combating Terrorism: State and USAID Should Improve Sustainability Planning for Key Counter-Terrorism Programs in Africa and the Middle East*, GAO-23-105442 (Washington, DC: September 2023).
[53] ODNI, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: ODNI, February 7, 2022), 7–8; ODNI, Annual Threat Assessment (February 5, 2024), 9–11.

Inside Russia's Proxy Ecosystem

Proxy Curators and Handlers Within the Russian State

By Eginhards Volāns

Since the full-scale invasion of Ukraine, Russia has escalated hybrid threats against Europe by testing its limits and thresholds, a dynamic that Eerik Kross and Greg Mills of the Royal United Services Institute have cleverly compared to a frog being slowly boiled in a pot.[1] Closer inspection shows that most of Russia's activities have been conducted through the use of various proxies – non-state actors leveraged by Moscow, that provide plausible deniability, complicate attribution, and delay Western countermeasures.

This reliance on proxies has long been embedded in the Russian regime and in how it pursues its objectives, both domestically and internationally. Whether by using Cossack groups to harass domestic opposition in Russia, destabilizing neighboring Estonia through pro-Russian movements like *Nochnoy Dozor*, initiating war in eastern Ukraine through pro-Russian separatists, or, more recently, conducting sabotage across Europe through the so-called "disposable agents."[2]

While the Kremlin has consistently insisted that it is not involved in any of these cases, the proxies behind them have rarely been autonomous and have instead been coordinated by the Russian state. Nevertheless, due to the inherent lack of transparency within the Russian government, understanding of the key Russian institutions responsible for orchestrating proxies remains limited. Mapping curators and handlers operating within the cabinets and corridors of Russian power should therefore be the first step in developing an effective policy to counter the hostile actions of their proxies.[3]

This article aims to bring some clarity on the issue and delves deeper into the initial findings presented in the European Centre of Excellence (CoE) for Countering Hybrid Threats (Hybrid CoE) Handbook on the Role of Non-State Actors in Russian Hybrid Threats, which was developed in the course of 2025.[4] It aims to deepen the understanding of the key Russian state institutions involved in the orchestration of proxies and provide

Eginhards Volāns is a senior analyst at the European Centre of Excellence (CoE) for Countering Hybrid Threats (Hybrid CoE) in Helsinki. His current focus is on the role of non-state actors in hybrid threats, with a particular emphasis on the use of proxies in Russian hybrid threat operations. He also co-leads Hybrid CoE's hybrid threat monitoring team, which tracks major incidents and analyzes the evolving hybrid threat environment.

answers to several research questions: (1) Which state institutions are primarily involved in orchestrating proxies? (2) Is there a clear hierarchy to how Russia manages these proxies? (3) To what extent are proxy activities coordinated across these institutions? (4) How has this system evolved since the full-scale invasion of Ukraine, and how is it likely to develop in the future?

Three distinct categories of proxies orchestrated by the Russian state are identified and mentioned in the article: armed proxies, which primarily provide the regime with kinetic power; cyber proxies, which deliver cyber capabilities; and influence proxies, which project pro-Russian narratives and soft power. While other proxy actors are also leveraged, these are the categories in which the state has the greatest capacity.

The article begins by presenting several points on the overall assessment of how proxy orchestration in Russia operates and has evolved over time, addressing some of the research questions outlined above. It then outlines several key state institutions involved in proxy orchestration and illustrates their roles with relevant, well-documented examples. The final section of the article examines the future of proxy orchestration and the possible directions it may take.

Overall Assessment

The use of proxies to target and weaken one's adversaries is nothing new. State reliance on proxies is, in fact, as old as states themselves, and, as noted by Vladimir Rauta, subversive activities by state-sponsored proxies are a staple of the "grey-zone operator's strategic toolbox."[5] Mercenaryism, sometimes referred to as the "world's second-oldest profession," and its use throughout history provide an illustrative case study to prove this point.[6] While today it is most commonly associated with rogue actors such as the Wagner Group, historically, it has been integral to state military power. In antiquity, Greek tyrants hired mercenaries from other city-states to serve as bodyguards, while during the Punic Wars, Carthage's armies were composed largely of foreign mercenaries. During the Middle Ages, Norse warriors, the Varangians, were an elite unit in the Byzantine Empire, while during the Renaissance, Italian city-states secured their interests primarily through hired armies and generals.

This is particularly true when examining the history of the Russian state, as its reliance on various proxy actors dates back to the Tsarist era. Some examples include the use of Cossack communities along the southern and eastern frontiers of the empire, or the reliance on the wealthy merchant and industrialist Stroganov family during the colonization of Siberia, or the use of monarchist and antisemitic groups with alleged ties to the Tsar's security apparatus, known as the Black Hundreds, to suppress the Revolution of 1905.

While these are valid and illustrative examples, the use of proxies in Tsarist Russia was largely opportunistic and can hardly be described as a coherent strategy. This changed after the establishment of Soviet rule and was further pioneered and perfected by the KGB during the Cold War.[7] During this period, the KGB significantly expanded the range of proxies in the service of the Kremlin, ranging from left-wing and Islamist militant groups to Western academia, university students, journalists, and social and political activists. The KGB effectively placed the use of proxies at the center of what today can be described as Russian hybrid threats. Modern-day Russia has not only adapted these tactics but also built on the same proxy networks once established by the KGB and the communist regime, using them to revitalize the Kremlin's influence worldwide in the 21st century.[8]

Today, the Russian state under Vladimir Putin's rule is characterized by informal relations between government bodies and various proxy networks closely linked to them. State and elite interests are

often intertwined with practices of personal enrichment, patronage, and informal power structures. As a result, the system resembles certain aspects of an organized criminal group and is therefore often described as a "mafia state."[9] In such an informal environment, ties between the state and their non-state proxies remain close but are not formalized in documents or agreements, and no clear boundaries are established.

As a result, information operations can be outsourced to private public relations companies such as the Social Design Agency (SDA), whose leadership has close ties to the Russian government, and their activities are *de facto* planned and coordinated within the Presidential Administration (AP).[10] At the same time, military operations can be outsourced to private military companies (PMCs) such as the Wagner Group or Moran Security Group, both founded by former Russian intelligence and security services (RISS) officers[11] Meanwhile, cyberattacks can be outsourced to cybercriminal gangs such as *REvil*, coerced and sanctioned by the same state institutions that are tasked with countering cybercrime.[12] The situation is further complicated by the widespread use of *dual delegation*, in which various intermediaries, such as the Orthodox Church or oligarchs, exercise actual control over the proxy rather than the state institutions themselves.[13]

Since the full-scale invasion of Ukraine, these ties have become even more difficult to trace, as Russia has significantly expanded censorship and eliminated most meaningful public reporting on the issue, reducing a lot of outside visibility into the regime's inner workings. As a result, analysis of the issue has become increasingly complex, and the overall external understanding of Russia's political and power dynamics has deteriorated. Furthermore, Western analysis, in particular, often overstates the degree of coordination and hierarchy within the Russian regime. As Stephen Hutchings and Joanna Szostek have concluded, "Russia is not the Soviet Union," and there is often an embedded lack of clear divisions of responsibility among its government bodies.[14] This means that in practice, decision-making in Russia is often *ad hoc*, state institutions lack a coherent strategy, and competition among various government bodies and influential figures is common. This dynamic is particularly evident among the always-competitive RISS and perhaps best illustrated by the rivalries among their cyber proxies.[15]

At the same time, it is worth noting that, despite ongoing competition, control over some proxy actors may be shared among multiple state institutions simultaneously. For example, while the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) is known to work closely with armed proxies, including paramilitary groups, militias, and right-wing extremists, so does the Federal Security Service (FSB). Furthermore, FSB's influence operations often overlap and are integrated with the Foreign Intelligence Service's (SVR), with both sharing some proxies and, in some cases, even the intelligence personnel handling them.[16] Nevertheless, *collective delegation* does not necessarily imply coordination among handlers. In practice, a single proxy may maintain parallel ties with multiple state institutions without their knowledge and use them to advance its own objectives.

As a result, there has been a gradual effort to centralize and increase coordination among various stakeholders within the Presidential Administration (PA) for some time now. Following the MH17 tragedy in 2014, the PA took the lead in minimizing its effects by establishing a dedicated task force and coordinating the activities of state institutions, mass media, and "internet trolls." The PA later played a similar role in minimizing the backlash from the so-called "Lisa case" in Germany.[17] Since the full-scale invasion of Ukraine, the centralization process has become even more vital and seems to have accelerated, with many of

Russia's proxy operations increasingly overseen by the First Deputy Chief of Staff of the PA, Sergey Kiriyenko, and his associates.[18]

The motivations behind proxy activities are often varied, ranging from ideological alignment to financial gain, or a combination of both. More importantly, these motivations are fluid and can shift over time. Actors, initially driven by ideology, may become motivated by financial gain, and vice versa. This dynamic is best exemplified by the shifting motivations of various hacktivist groups and cybercriminals operating on the Kremlin's behalf.[19] Furthermore, Western analysis often overstates the importance of ideological motivation in the case of Russian proxies. Many influence proxies, ranging from journalists to opinion leaders, are primarily motivated by financial gain and use ideology only as a public pretext for their actions. This is exemplified by leaked documents from the Kremlin, in which officials have complained that "no one wants to be friends with Russia for free."[20]

Fluidity can also be observed in proxy handlers, tasks, and even operational regions. This dynamic is evident in the case of Russian proxies involved in the destabilization of Estonia during the Bronze Night riots in 2007. For example, Dmitry Linter, one of the leaders of the *Nochnoy Dozor* movement, was later involved in the formation of "volunteer units" during the annexation of Crimea and subsequently pursued a political career in the occupied Donetsk People's Republic.[21] Meanwhile, Linter's comrade-in-arms, Maxim Reva, shifted his regional focus entirely and is now the deputy head of the RISS-affiliated African Initiative project, which is tasked with spreading disinformation and Russian influence in Africa.[22] Another Russian proxy active in Estonia, Alik Khuchbarov, was convicted of collaborating with the FSB in 2016, yet by 2024 had changed his handlers and was reportedly carrying out sabotage operations on behalf of the GRU.[23]

Since 2022, Russia's international isolation and Western countermeasures, such as the expulsion of diplomatic staff and RISS officers operating under diplomatic cover, have significantly altered the recruitment and management of proxies abroad. This has led to the identification and recruitment of new proxy actors through online platforms and the so-called gig economy, resulting in looser control over their activities.[24] The increased lack of direct state control is exemplified by recent studies on Russia's use of "disposable agents," which have found that only 58% of perpetrators were aware that their actions were directed by RISS, as many were recruited through intermediaries such as PMCs and transnational criminal networks (TCNs).[25]

At the same time, Russia appears to be relying increasingly on senior political, economic, and bureaucratic figures within target states to conceal its involvement. These actors, who possess their own patronage networks and intermediaries in targeted countries, serve as indirect and legitimate proxies for the Kremlin. As a result, lower-level agents operating within these networks may be unaware of Russia's involvement altogether, believing they are acting on behalf of local actors, even when their activities are fully aligned with Russian strategic objectives.[26]

Key State Institutions Behind Proxies

Russia's proxy landscape is vast and complex, involving a wide range of state actors that are often intertwined, interlinked, and at times in competition with one another. While efforts to map this phenomenon have been undertaken by various organizations and experts, much work remains to achieve a comprehensive understanding of its scope.[27] As the entire Russian state apparatus is too extensive to be described in a single article, the text will instead focus on two distinct yet closely connected centers of power most involved in the orchestration of proxies. First, it will examine the

strategic overseers of the proxies in the PA. Second, it will explore the actual handlers of proxies within the security apparatus, the so-called *siloviki*, in particular the GRU, FSB, SVR, and the Federal Service of Troops of National Guard (*Rosgvardiya*).

The Presidential Administration

As noted by Mark Galeotti, while the Russian political system is largely an informal one, the closest thing to a true command-and-control nexus, including for non-military interference abroad, can be found in the PA.[28] That said, with regard to proxy operations, three directorates need to be discussed: (1) Directorate for Interregional and Cultural Relations with Foreign Countries, (2) Directorate for Cross-Border Cooperation and (3) Directorate for Strategic Partnership and Cooperation.[29]

Before the restructuring, Directorates for Interregional and Cultural Relations and for Cross-Border Cooperation were known as the PA's key structures for establishing and operating extensive influence proxy networks designed to influence and destabilize Russia's so-called "near abroad." The directorates also maintained significant ties with RISS, with former officers working in them. As of the writing of this article, their personnel, tasks and operational regions are inherited by the newly established Directorate for Strategic Partnership and Cooperation.[30]

While these directorates no longer exist, they provide the most valuable source material for understanding how proxy orchestration has been conducted within the PA and therefore require deeper analysis.

The Directorates for Influencing Russia's "Near Abroad"

The **Directorate for Interregional and Cultural Relations with Foreign Countries** was established in 2005, and its creation was likely in response to the so-called "color revolutions" in Georgia (2003), Ukraine (2004), and Kyrgyzstan (2005), and aimed at restoring Russia's declining influence in the post-Soviet space. This marked the first shift toward the professionalization and centralization of influence proxy use within the PA and foreign influence operations more broadly. The **Directorate for Cross-Border Cooperation** was established later in 2018 with the aim of exerting influence over Ukraine's self-proclaimed separatist republics, the Georgian breakaway regions of Abkhazia and South Ossetia, as well as Moldova's breakaway region of Transnistria.31 This marked the second shift toward greater professionalization and specialization.

Both departments had a strong presence of RISS officers, particularly, from the SVR, and had developed extensive networks of proxies aimed at influencing, and, if necessary, destabilizing, former Soviet states. Their agents were highly active across informational, cultural, social, and political domains of countries like Latvia, Moldova and Georgia as illustrated in Table 1.

In addition to operating proxy networks, the directorates were involved in developing foresight strategies for the PA. For example, in late 2021, the Directorate for Cross-Border Cooperation produced a roadmap that envisioned the absorption of Belarus by Russia by 2030. The document discussed the promotion of pro-Russian figures within the Belarusian political and military establishment, as well as the increased presence of Russian media in the country.[32] Around the same time, the directorate drafted another 10-year strategy aimed at undermining Moldova's efforts toward Western integration. The strategy discussed the creation of pro-Russian NGOs, influencing Moldovan youth, and the formation of pro-Russian groups among Moldova's political and economic elites.[33]

Table 1: Types of Influence Proxies Managed by the Directorate for Interregional and Cultural Relations with Foreign Countries and the Directorate for Cross-Border Cooperation.

Opinion Leaders	Political Parties	NGOs	Media
Numerous propagandists, experts, and other opinion leaders were handled by the RISS personnel stationed in the directorates in order to shape public opinions. For example, the former curator of the Baltic file within the Directorate, Yevgeniy Umerenkov, worked closely with journalists from the popular Russian newspaper Komsomolskaya Pravda.	Political parties and individual politicians were backed, supervised and financed by the directorate. For example, the Moldova file was headed by Igor Maslov, a former SVR resident in the Balkans, who was in close contact with the pro-Russian ex-president of Moldova, Igor Dodon. In Georgia, Russian influence was managed through the Georgian Alliance of Patriots, which was supervised by the Moscow-based firm POLITSECRETS, which was in turn guided by the PA.	The directorates handled multiple NGOs whose operations ranged from supporting Russian compatriot rights to promotion of Russian culture and historical revisionism. For example, the Historical Memory Foundation was used as a front to operate a network of more than a dozen NGOs.	The directorates established and financed full-fledged media sources like the Latvian and Belarussian versions of IMHO Club or the Baltic-oriented analytical news portal RuBaltic, which were used to employ and pay local journalists for spreading pro-Russian propaganda.

Source: Author.

Sources referenced in the Table 1: "Kak Kreml vmeshivaetsya vo vnutrenniuiu politiku sosednikh stran," Dossier Center, November 25, 2020, https://dossier.center/pribaltika/; Kanev, "Spies, Banquets, and Embezzlement."; Will Neal, "NGO Probe Finds Russia 'Directly Influencing' Georgian Politics," OCCRP, September 1, 2020, www.occrp.org/en/news/ngo-probe-finds-russia-directly-influencing-georgian-politics; *Otchet o deyatelnosti fonda Istoricheskaya pamyat za 2008-2019 gg*, Leaked Documents (Dossier Center, 2020), https://dossier.center/wp-content/uploads/2020/11/24-prib-sldfjs8slfn.pdf; RuBaltic was used as an intermediary to build proxy networks of influence agents in the Baltic region, organizing seminars for local journalists and employing some of them to produce pro-Kremlin propaganda content. See: "Noplūdušā e-pastu sarakstē atrodami Krievijā tapuši plāni, kā nomelnot Vienotību," TV3, December 20, 2020, www.tv3.lv/zinas/latvija/neka-personiga/nopludusa-e-pastu-sarakste-atrodami-krievija-tapusi-plani-ka-nomelnot-vienotibu/.

After two decades of sustained operations and significant financial investment, by 2025, it had become clear that Russia's policy toward its so-called "near abroad" had largely failed. Following the full-scale invasion of Ukraine, Moscow's influence continued to dwindle at an unprecedented scale. Russia lost much of already limited leverage it had in the Baltic states, increasingly lost influence over Armenia, and faced the potential erosion of its influence in Central Asia, particularly in Kazakhstan.[34] Furthermore, it is important to note that the two directorates were overseen by Dmitry Kozak, a long serving aid to Putin, who had gradually lost his influence after the full-scale invasion, which he reportedly saw as a mistake.[35]

These two aspects likely prompted the dismantlement of the two directorates and the establishment of the new **Directorate for Strategic Partnership and Cooperation** in August 2025.[36] In October 2025, a new head, Vadim Titov, was appointed to lead the newly established directorate. Titov had prior professional ties with the First Deputy Chief of Staff of the PA, Kiriyenko, and can be viewed as his protégé. This suggests that Kiriyenko has consolidated his position within the PA and emerged as a central figure in the broader management of proxy operations abroad.[37] The tasks of the newly established directorate have nonetheless remained unchanged: extending the Kremlin's presence abroad primarily through influence agents and covert operations.[38]

It is worth addressing that since 2022, Kiriyenko in particular has played an increasingly central role in the Kremlin's operations aimed at shaping and altering Western decision-making, with private companies such as SDA and *Struktura* conducting global disinformation operations under his direct supervision.[39] Ukrainian military intelligence has also suspected Kiriyenko's direct involvement in the "Maidan-3" operation aimed at overthrowing President Volodymyr Zelensky in 2024.[40] Even before becoming the curator of the Directorate for Strategic Partnership and Cooperation, his name has been linked to organizing election interference in Abkhazia, Moldova and Armenia.[41] It can be anticipated that such operations under Kiriyenko's guidance will adopt a broader geographic focus beyond the so-called "near abroad," possibly extending to regions like Africa, a portfolio that has already been assigned to him following Yevgeniy Prigozhin's mutiny.[42]

Other changes may be observed in the replacement of traditional, more rigid intelligence-led tactics prevalent in previous decades with a more private sector-oriented approach, similar to that seen in Kiriyenko's domestic policy initiatives in Russia.[43] Additionally, greater centralization and stronger interlinkages between domestic and foreign policy blocks could emerge, as directorates under Kiriyenko's supervision that are responsible for domestic issues might be integrated into a wider system of influence.[44]

Main Directorate of the General Staff of the Armed Forces of the Russian Federation

The GRU plays a key role in orchestrating various armed proxies and is probably best known for its ties to PMCs and various paramilitary formations and militias.[45] The GRU's direct control over armed proxies has likely expanded significantly since the invasion of Ukraine, and even further in the aftermath of Prigozhin's mutiny.[46] For example, the GRU exercises control over the Redut PMC, a former competitor of the Wagner Group.[47] Redut functions as an umbrella organization for more than 20-armed formations with a combined manpower of tens of thousands. Its fighters are paid directly by the Ministry of Defense, led by GRU officers, and assigned to covert military units. As a result, Redut possesses little independent agency and operates in practice as a state-run program.[48] The GRU has also taken over much of Russia's military presence in Africa and oversees previous Wagner Groups operations on the continent. The Africa Corps has emerged as a key proxy of the GRU on the continent. It is led by Andrey Averyanov, the former head of the infamous 161st Specialist Training Center (military unit 29155), which, among other tasks, is also responsible for diversions and sabotages across Europe in the aftermath of the invasion of Ukraine.[49]

In addition to the tightly controlled PMCs, GRU is known for its contacts to various far right extremist groups that can also be leveraged in covert operations. One such organization is the Russian Imperial Movement, which gained notoriety for

sending letter bombs in Spain in 2022/2023.[50] The GRU has also reportedly employed neo-Nazi figures, such as Yevgeniy Rasskazov, to lead its online agent recruitment campaigns.[51]

Since the full-scale invasion of Ukraine, the aforementioned **161st Specialist Training Center** has become a key orchestrator of various sabotage and diversion operations across Europe through a mix of locally hired criminals and "useful idiots," often recruited on social media platforms like Telegram.[52] These recruits are often inexperienced and unprofessional, reflecting a new approach that prioritizes quantity over quality. As described by an anonymous European security official: "you jail one person, and another pops up to take their place. These people are disposable, and Moscow doesn't care about them."[53] GRU's growing reliance on such proxy agents likely stems from the expulsion of actual intelligence officers from Europe after the full-scale invasion.[54]

As of spring 2026, GRU is also reported to be linked to **Center 795** (military unit 75127), which was established in 2023 and is tasked with organising political assassinations and kidnappings abroad. The unit is reportedly based at a training centre associated with Kalashnikov Concern and financed by private actors, including the oligarch Andrey Bokarev, resembling a pattern similar to that of the Wagner Group under Yevgeny Prigozhin. While Center 795 itself is not a proxy in a traditional sense, it is involved in the recruitment of foreign proxy agents, as illustrated by its exposure after its officers reportedly used Google Translate to communicate with a recruit from Serbia.[55]

Furthermore, while TCNs have traditionally fallen under the portfolio of FSB, influential criminal figures such as the arms dealer Viktor Bout have been reported to maintain connections with GRU as well. Moreover, Viktor Bout has been cited as a possible intermediary between the GRU and the Houthi terrorists in Yemen. It is also worth noting that GRU has been reportedly operating in Houthi-controlled territory under the guise of humanitarian aid, establishing potential ties with radical Islamists and creating potential openings for ties between Russia and Islamists.[56]

In addition to overseeing armed proxies, GRU has significant capabilities regarding influence and cyber operations. Its key psychological operations division is the **72nd Special Service Center** (military unit 54777), which relies heavily on various front organizations, such as the Institute of the Russian Diaspora and *InfoRos*, the latter of which has been involved in setting up

Table 2: GRU Structures Responsible for Orchestrating Cyber Proxies.

85th Main Special Service Center (military unit 26165)	**Main Center for Special Technologies** (military unit 744555)	**161st Specialist Training Center** (military unit 29155)
Controls the APT28 group (also known as Fancy Bear, Pawn Storm, Strontium, Sofacy, Forest Blizzard).	Operates the Sandworm group (also known as Telebots, Voodoo Bear, IRIDIUM, Seashell Blizzard, Iron Viking), which is also GRU's key intermediary for pro-Russian hacktivist collectives such as the XakNet Team, Cyber Army of Russia Reborn and Solntsepek.	Controls the Ember Bear group (also known as Cadet Blizzard, Bleeding Bear). Potentially outsources some of its operations to cybercriminals.

Source: Author.

approximately 1,300 proxy websites in the Russian language alone.[57] Additionally, the aforementioned 161st Special Training Center is linked to the coordination of multiple information operations collectively known as Storm-1516, which is possibly operated by the Center for Geopolitical Expertise, a think tank with links to ideologue Aleksandr Dugin.[58]

Moreover, the GRU runs an extensive offensive cyber program, and several of its structures are involved in controlling or overseeing cyber proxies, including directly controlled advanced persistent threat (APT) groups, hacktivist collectives and cybercriminals. Particular GRU structures and their cyber proxies are discussed in Table 2.

Federal Security Service

The FSB is well known for leveraging both domestic and international proxies. The most prominent structure dedicated to influencing and destabilizing foreign states is the FSB's **Service for Operational Information and International Relations** (Fifth Service), which oversees both international operations as well as intelligence analysis.[59] During the Soviet times its predecessor, KGB's Fifth Service, was responsible for counter-intelligence in the non-Russian Soviet republics. As a result, it inherited a vast network of agents around the post-Soviet republics, useful for both espionage and influence.[60] As of today, it has been involved in operations across Russia's "near abroad," including Moldova and Ukraine, but also in Western European states such as France, Italy, and Germany.[61] The Fifth Service is also involved in operations in Africa, relying on proxy media outlets, covert social media networks, and local intermediaries.[62] As part of its analytical role, the Fifth Service is also believed to be responsible for providing inaccurate and biased assessments of the situation in Ukraine, which guided Putin's decision to launch a full-scale invasion in 2022.[63]

Furthermore, FSB's **Service for the Protection of the Constitutional Order and Combating Terrorism** (Second Service) has also been involved in similar operations abroad.[64] Proxy-related operations of the Second Service are best exemplified by the case of Aleksandr Ionov, a pro-Kremlin activist who acted as an FSB intermediary, coordinating propaganda narratives, political contacts, and financial support, allegedly in the U.S.[65] Apart from that the Second Service also reportedly caries out political repressions against Russia's opposition and as of spring 2026, is reportedly the key entity overseeing the extensive censorship crackdown on the Russian internet segment.[66]

In addition, the FSB has been involved in operating multiple proxy websites to disseminate propaganda and disinformation, most prominently *NewsFront* and *SouthFront*.[67] It is also well known for using private companies as fronts. For example, it has been linked to maritime and dredging companies operating from the ports of Latvia and Lithuania.[68] Because of its business connections, the FSB plays an important role in Russian sanctions evasion and procurement schemes.[69] Furthermore, it is also known for its close ties to domestic Russian far-right extremist groups such as *Russkaya Obshchina* and *Rusich*, with the latter involved in joint missions with the FSB-led Russian Border Guard.[70]

The FSB is probably best known for its ties to TCNs, a practice rooted in the Soviet period and the KGB's long-standing use of criminals as instruments of domestic intelligence.[71] As the FSB is in control of Russia's Border Guard, it is also overseeing TCNs involved in smuggling activities.[72] During Putin's rule, the FSB has also become associated with state-ordered assassinations carried out by contract killers, with the most notable example being Vadim Krasikov.[73]

Furthermore, the FSB is also known for its close ties to the cybercriminal underworld, with many hackers operating as contractors within its cyber units and conducting attacks against the

Table 3: FSB Structures Responsible for Orchestrating Cyber Proxies

16th Center (military unit 71330)	18th Center (military unit 64829)
Known for operating one of the oldest and most sophisticated hacking groups in Russia's arsenal Turla (also known as Snake, Venomous Bear, Secret Blizzard) as well as the Energetic Bear (also known as (Energetic Bear, Ghost Blizzard, Crouching Yeti).	Controls Gamaredon (also known as Primitive Bear) and Callisto (Seaborgium, Coldriver, Star Blizzard) hacking groups. Additionally, while officially serving as FSB's cybercrime unit, the 18th Center is also known for recruiting and overseeing cybercriminals.

Source: Author.

Kremlin's adversaries worldwide. Particular FSB structures and their cyber proxies are discussed in Table 3.

Foreign Intelligence Service

While historically concentrated on traditional espionage, the SVR has expanded its toolkit to include the cultivation and deployment of proxy agents for operations abroad as well. In particular, the SVR has established itself as a key institution for managing proxies involved in foreign influence such as various government NGOs (GONGOs), NGOs and think tanks.[74] The SVR is also known for its close ties to the journalistic community and for maintaining its own cyber proxies.

Most notably, the Russian Institute for Strategic Studies, a pro-Kremlin think tank staffed by former SVR officers, has been linked to the alleged election interference in the U.S. and the promotion of conservative, anti-liberal, and anti-Ukrainian narratives.[75] Additionally, the Foundation for Support and Protection of the Rights of Compatriots Living Abroad (*Pravfond*), formally tasked with providing legal assistance to Russian compatriots, is also reportedly staffed by former SVR officers and has been used as a front organization in at least 48 countries.[76] Further, the Federal Agency for the Commonwealth of Independent States Affairs, Compatriots Living Abroad, and International Humanitarian Cooperation (*Rossotrudnichestvo*), which is tasked with projecting Russian soft power abroad, is also used as a cover for officers from the SVR and other RISS.[77] These organizations are often used as intermediaries to recruit, finance and orchestrate various other influence proxies abroad.

The SVR also deploys its officers under journalistic cover, often through the state-linked news agency *TASS*. By operating under cover, SVR can conduct espionage and facilitate access to broader proxy networks within the global media community.[78] Similar practices were employed by the SVR's predecessor, the KGB, during the Cold War.[79] Additionally, the SVR is also known to operate multiple proxy websites, with the most prominent examples being *Strategic Culture Foundation*, *New Eastern Outlook*, and *Oriental Review*.[80] It is also involved in covert influence operations such as Kylo, aimed at damaging social cohesion in Europe, and Ledorub, aimed at disrupting Russian opposition activities abroad.[81] As of spring 2026, the SVR is reportedly overseeing the political technology assets formerly associated with Prigozhin, known as "The Company," which are used to expand Russian influence in the Global South.[82] It also oversees the APT29 hacking group (also known as Cozy Bear, The Dukes, Midnight Blizzard), which has conducted major cyberespionage operations, including the 2020 SolarWinds hack.[83]

Federal Service of Troops of National Guard

Established in 2016 and sometimes described as Putin's "praetorian guard," *Rosgvardiya* is tasked with maintaining public order and security, or in other words, suppressing opposition and protests, guarding key government facilities and critical infrastructure, participating in counterterrorism operations, and protecting certain senior officials.[84] Since 2022, it has been involved in enforcing Russian occupation regime in Ukrainian territories under Moscow's control.[85]

Rosgvardiya is also known to operate as an umbrella organization for several Kremlin-aligned armed proxies. It has been linked, for example, to domestic militias such as the Cossack movement, which refers to a loose constellation of organizations claiming cultural and historical heritage with Tsarist-era Cossack communities. In 2021, it was reported that dedicated Cossack units would be formally established under *Rosgvardiya*.[86] Cossacks have been traditionally involved in supporting border control, maintaining public order, and suppressing dissent. According to official figures, there are approximately 140,000 registered Cossacks in Russia, around 50,000 of whom have participated in the war in Ukraine. During the invasion of Ukraine, Cossack forces assisted *Rosgvardiya* at checkpoints and filtration camps in occupied territories.[87] Cossack organizations also maintain close ties with the police and regular military forces.[88]

Another example is *Kadyrovtsy*, the personal militia of Chechnya's dictator Ramzan Kadyrov. While *Kadyrovtsy* possess significantly more agency than the Cossacks or many other armed proxies employed by the Russian regime, and effectively act as Kadyrov's personal army, they are formally placed under the umbrella of *Rosgvardiya*.[89] *Kadyrovtsy* are widely known for their brutality and for operating outside legal frameworks, including carrying out extrajudicial executions of dissidents in Chechnya.[90] Additionally, some of the fighters from the Wagner Group have been absorbed into *Kadyrovtsy* after the 2023 mutiny, while others have joined the newly legalized Volunteer Corps under *Rosgvardiya*,[91] with the latter reportedly led by Prigozhin's son Pavel.[92] Their role and degree of subordination remain unclear, and publicly available information on the remnants of the Wagner Group now operating under *Rosgvardiya* is scarce.

Outlook

Based on the analysis presented in the article, three key conclusions can be made about the likely future evolution of Russia's proxy ecosystem, state institutions behind it, and Russian proxy operations in general.

First, **Russia's isolation and radicalization is accelerating its reliance on proxies**. The Kremlin's reliance on proxies has increased since the start of the full-scale war in Ukraine and is expected to continue growing. Domestically, the war has accelerated Russia's shift toward a more autocratic, even totalitarian, political system, with the state expanding its involvement across nearly all areas of everyday life. All non-state actors, ranging from private businesses to armed groups, have been pushed under more direct and strict regime control. This expansion into the private sector is largely enforced through coercion, intimidation, and blackmail. Internationally, Russia has been constrained by Western sanctions, the expulsion of Russian diplomats, and the blocking of Russian state media, which have reduced the effectiveness of traditional state instruments and increased the regime's reliance on proxy actors operating abroad. As a result, the use of "disposable agents," foreign opinion leaders, and various front companies has become essential for sustaining Kremlin's operations abroad. At the same time, proxies such as TCNs, hackers, and armed groups likely view the war in Ukraine and the growing

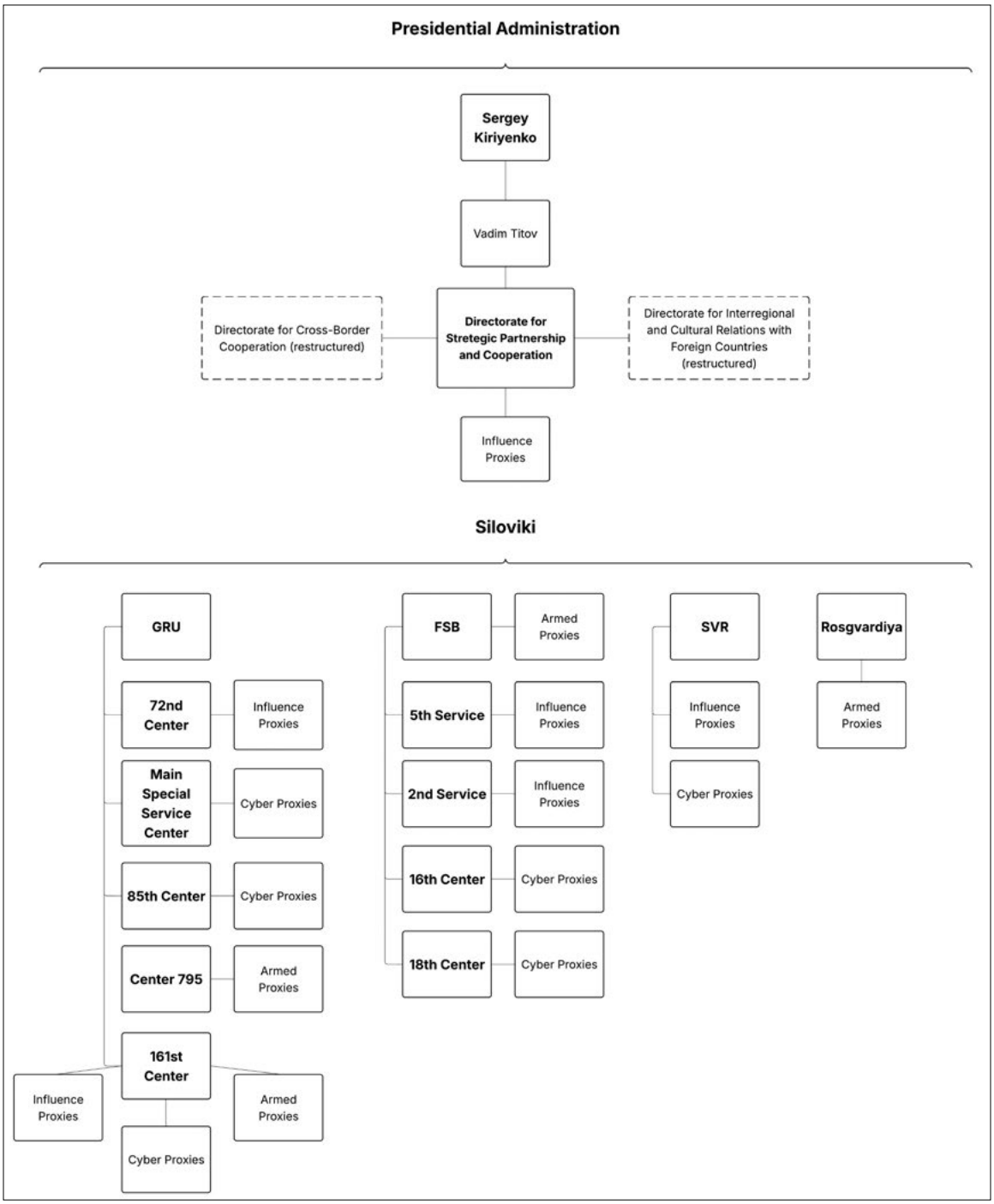
confrontation with the West as a window of opportunity to strengthen their own positions and secure financial or political benefits, as the state becomes more dependent on their services.

Second, **Russia's proxy operations have the potential to become more professional, centralized, and effective.** As proxy orchestration becomes increasingly concentrated and centralized within the PA, and seemingly under Kiriyenko, there is a growing concern that Russian operations will become more professionalized, centralized and ultimately more effective. Kiriyenko has built a reputation as an efficient and adaptable government manager who has strengthened Putin's grip on power through propaganda, influence, and censorship. His approach as the curator of the Kremlin's domestic policy block proved effective by prioritizing private sector techniques over traditional intelligence tactics. His model emphasized the use of political technologists, outsourcing to private actors, and the application of marketing techniques to achieve political objectives. These methods contrast with the more rigid practices traditionally employed by RISS. If applied to external activities, this model could reshape how Russia's proxy operations are conducted. By supplementing, or partially replacing, traditional RISS-led approaches with private-sector expertise, Kiriyenko's framework may lead to a more flexible, deniable, and professionally managed proxy networks, that can enhance Russia's capacity to project influence abroad.

Third, **new internal power struggles could emerge, halting the centralization processes.** Structural changes in the PA introduced by Putin in the second half of 2025, including the dismissal of Kozak as the curator of the PA's influence operations abroad and the restructuring of his subordinate directorates, largely staffed by RISS officers and responsible for RISS-led proxy networks, may trigger new inter-institutional competition. The Russian system is well known for its internal power struggles between various centers of authority, the so-called "towers of the Kremlin." The recent changes in the PA and the growing prominence of Kiriyenko may therefore result in new tensions between him and his close associates among political technologists and private-sector appointees, on the one hand, and the traditional, RISS-dominated siloviki, on the other.

Appendix

Russian State Institutions Involved in the Orchestration of Proxies.



Source: Author.

Endnotes

[1] Kross, Eerik and Greg Mills, "A Frog in a Pot – Turning Around Russia's Hybrid War," *RUSI*, October 22, 2025, https://www.rusi.org/explore-our-research/publications/commentary/frog-pot-turning-around-russias-hybrid-war.
[2] Kazdobina, Julia, Jakob Hedenskog, and Andreas Umland, *Why the Donbas War Was Never Civil*, SCEEUS Report No. 6 (Stockholm: Stockholm Centre for Eastern European Studies, April 12, 2024), 4, https://www.ui.se/globalassets/ui.se-eng/publications/other-publications/why-the-donbas-war-was-never-civil-sceeus-report-no6-2024.pdf; Luke Harding, "WikiLeaks Cables Claim Russia Armed Georgian Separatists," *The Guardian*, December 1, 2010, https://www.theguardian.com/world/2010/dec/01/wikileaks-cables-russia-georgian-separatists; Vladimir Socor, "Red Army Monument Removed from Tallinn amid Moscow-Encouraged Riots," *Eurasia Daily Monitor*, May 2, 2007, https://jamestown.org/red-army-monument-removed-from-tallinn-amid-moscow-encouraged-riots/; Andrew Roth, "4 Things You Need to Know About the Cossacks Fighting Russia's Opposition Groups," *The Washington Post*, May 18, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/05/18/4-things-you-need-to-know-about-the-cossacks-fighting-russias-opposition-groups/; Rekawek, Kacper, Julian Lanchès, Maria Zotova, and Donald Bowser, *Russia's Crime–Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe*, (GLOBSEC and International Centre for Counter-Terrorism, 2025), 21, https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf.
[3] Vladimir Rauta, *Countering state-sponsored proxies: designing a robust policy*, Hybrid CoE Paper 23 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2025), 11, https://www.hybridcoe.fi/wp-content/uploads/2025/02/web_Hybrid_CoE_Paper-23_rgb.pdf.
[4] Volāns, Eginhards, Vladimir Rauta, Magda Long, Andis Kudors, Agata Kleczkowska and Eliza Lockhart, *Handbook on the role of non-state actors in Russian hybrid threats*, Hybrid CoE Paper 27 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2025), https://www.hybridcoe.fi/wp-content/uploads/2025/12/Hybrid-CoE-Paper-27-Handbook-on-the-role-of-non-state-actors-in-Russian-hybrid-threats.pdf.
[5] Jokinen, Janne, Magnus Normark, and Michael Fredholm, *Hybrid threats from non-state actors: A taxonomy*, Hybrid CoE Research Report 6 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2022), 4, https://www.hybridcoe.fi/wp-content/uploads/2022/06/Hybrid-Coe-Research-Report-6-WEB-EDS-20221121.pdf; Rauta, *Countering state-sponsored proxies*, 4.
[6] Sarah Percy, *Mercenaries: The History of a Norm in International Relations* (Oxford: Oxford University Press, 2007).
[7] Mark Galeotti, "Active Measures: Russia's Covert Geopolitical Operations," *Marshall Center*, June 2019, https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0; Ivo Juurvee, *The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox*, Hybrid CoE Strategic Analysis *7*, (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2018), 3, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-analysis-7-April.pdf.
[8] Catherine Belton, *Putin's People: How the KGB Took Back Russia and Then Took on the West* (London: William Collins, 2020).
[9] Munira Mustaffa, "Russia: The mafia as the state," *Lowy Institute*, August 31, 2023, https://www.lowyinstitute.org/the-interpreter/russia-mafia-state.
[10] Grigory Asmolov, "Propaganda v setevoy srede: kak menyalas propaganda v epokhu sotsialnykh media i v usloviyakh voyny," *Re:Russia*, April 5, 2024. https://re-russia.net/expertise/714/; Matthew Kupfer, "Investigation: Who Is Ilya Gambashidze, the Man the US Government Accuses of Running a Kremlin Disinformation Campaign?," *Voice of America*, May 9, 2024, https://www.voanews.com/a/investigation-who-is-ilya-gambashidze-the-man-the-us-government-accuses-of-running-a-kremlin-disinformation-campaign-/7604052.html.
[11] Sean Seadon, "Who is Dmitry Utkin and who else was on the plane?," *BBC*, August 24, 2023, https://www.bbc.com/news/world-europe-6660275; Candace Rondeaux, *Decoding the Wagner Group: Analyzing the Role of Private Military Security Contractors in Russian Proxy Warfare* (New America, November 5, 2019), 41, https://d1y8sb8igg2f8e.cloudfront.net/documents/Decoding_the_Wagner_Group.pdf.
[12] *Dark Covenant 3.0: Controlled Impunity and Russia's Cybercriminals*, Cyber Threat Analysis Report (Recorded Future, October 22, 2025), 12, https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-ru-2025-1022.pdf.

[13] *Dual delegation* describes a process in which the delegation of authority is delegated to one agent who then further delegates this to another agent. See: Karlén, Niklas et al. "Forum: Conflict Delegation in Civil Wars," *International Studies Review* 23, No.4 (2021): 2060, https://academic.oup.com/isr/article/23/4/2048/6419778.
[14] Hutchings, Stephen and Joanna Szostek, "Dominant Narratives in Russian Political and Media Discourse During the Ukraine Crisis," in *Ukraine and Russia: People, Politics, Propaganda, and Perspectives*, ed. Pikulicka-Wilczewska, Agnieszka and Richard Sakwa (Bristol: E-International Relations, 2015), 179, https://www.e-ir.info/wp-content/uploads/2016/06/Ukraine-and-Russia-E-IR-2016.pdf.
[15] Melella, Cosimo, Francesco Ferazza, and Konstantinos Mersinas, "Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies," *Applied Cybersecurity & Internet Governance (ACIG) Journal* 4, No. 2 (2024): 1-2, https://www.researchgate.net/publication/383846195_Disjointed_Cyber_Warfare_Internal_Conflicts_among_Russian_Intelligence_Agencies.
[16] Dobrokhotov, Roman, Hristo Grozev and Michael Weis, "Soobrazheniyami morali i nravstvennosti prenebrech: kak SVR organizuet dezinformatsionnye kampanii na Zapade," *The Insider*, July 4, 2024, https://theins.ru/inv/272852.
[17] The "Lisa case" was a Russian disinformation operation in Germany in 2016 that falsely alleged the abduction and rape of a 13-year-old Russian German girl by migrants, with the aim of inflaming social tensions. See: Jakub Janda, *The Lisa Case. STRATCOM Lessons for European states*, Security Policy Working Paper No. 11/2016, (Federal Academy for Security Policy, 2016), https://www.baks.bund.de/sites/default/files/working_paper_2016_11.pdf; Mark Galeotti, "The Presidential Administration: The Command and Control Nexus of Putin's Russia," *Marshall Center*, February 2020, https://www.marshallcenter.org/en/publications/security-insights/presidential-administration-command-and-control-nexus-putins-russia-0.
[18] Andrey Pertsev, "What to Expect from the Kremlin's New Overseer of Post-Soviet States," *Carnegie Politika*, July 14, 2025, https://carnegieendowment.org/russia-eurasia/politika/2025/07/russia-post-soviet-politics?lang=en.
[19] For instance, Killnet hacktivist collective began as a purely ideological supporter of the Kremlin's geopolitical ambitions, yet over time it evolved into a cybercriminal-for-hire organization. See: "Evolution of KILLNET from Hacktivism to Private Hackers Company and the Role of Sub-groups," *CYFIRMA*, May 12, 2023, https://www.cyfirma.com/research/evolution-of-killnet-from-hacktivism-to-private-hackers-company-and-the-role-of-sub-groups/.
[20] Sergey Kanev, "Spies, Banquets, and Embezzlement: The Inner Workings of Putin's 'Cultural Ties' Directorate," *The Insider*, September 12, 2025, www.theins.ru/en/inv/284875.
[21] Dmitrii Durnev, "Drug Putina, ziat Pushilina. Kak Dmitrii Linter – chlen estonskoi "bronzovoi chetverki" – voshel v rukovodstvo DNR," *DELFI*, December 30, 2019, https://rus.delfi.ee/statja/88513047/drug-putina-zyat-pushilina-kak-dmitriy-linter-chlen-estonskoy-bronzovoy-chetverki-voshel-v-rukovodstvo-dnr.
[22] The African Initiative editorial board includes several individuals previously involved in influence operations in the post-Soviet countries. See: *African Initiative: From Public Diplomacy to Covert Influence Operations*, VIGINUM Technical Report, (France: SGDSN, 2025), 5, https://www.sgdsn.gouv.fr/files/files/Publications/20250612_TLP-CLEAR_VIGINUM_FCDO_EEAS_Technical_Report_African_Initiative_EN.pdf; *Annual Review 2024–2025* (Tallinn: KAPO, 2025), 27, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf.
[23] *Ibid*.
[24] Richterova, Daniela, Elena Grossfeld, Magda Long, and Patrick Bury, "Russian Sabotage in the Gig-Economy Era," *The RUSI Journal*, No.169 (2024): 10–21, https://www.tandfonline.com/doi/full/10.1080/03071847.2024.2401232.
[25] Rekawek et al., *Russia–Crime–Terror Nexus*, 24.
[26] Watling, Jack, Oleksandr V. Danylyuk, and Nick Reynolds, *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023* (London: RUSI, 2023), 6, https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.pdf.
[27] The exact typology of the various non-state actors used by Russia is described in detail by the Hybrid CoE. See: Volāns et.al., *Handbook on role of non-state actors in Russian hybrid threats*.
[28] Galeotti, "*The Presidential Administration: The Command and Control Nexus of Putin's Russia*."

[29] In 2025, the first two underwent significant restructuring and were effectively absorbed into the newly created Directorate for Strategic Partnership and Cooperation, which is likely to serve as the key structure for operating proxies abroad from now on. See: Andrey Pertsev, "Otkuda otstavka Dmitriya Kozaka i chto ona oznachaet dlya rossiyskoy politiki," *Carnegie Politika*, September 22, 2025, https://carnegieendowment.org/russia-eurasia/politika/2025/09/russia-kozak-resignation?lang=ru.

[30] "Chast tretya: general Chernov, kuratory i filbifily," *Dossier Center*, September 2, 2020, https://dossier.center/chernov/.

[31] Gielewska, Anna and Szabolcs Panyi, "How Russia Plans to Take Over Belarus," *VSquare*, February 20, 2023, https://vsquare.org/secret-kremlin-document-russia-plans-take-over-belarus-putin/.

[32] "V 2021 godu Kreml planiroval zahvatit ne tolko Ukrainu, no i Belarus – pravda postepenno," *Dossier Center*, February 20, 2023, https://dossier.center/union-br/.

[33] "Plan Kremlya dlya Moldovy," *RISE,* March 15, 2023, https://www.rise.md/rusa/%D0%BF%D0%B-B%D0%B0%D0%BD-%D0%BA%D1%80%D0%B5%D0%BC%D0%BB%D1%8F-%D0%B4%D0%B-B%D1%8F-%D0%BC%D0%BE%D0%B-B%D0%B4%D0%BE%D0%B2%D1%8B/.

[34] Jeffrey Mankoff, "Russia Is Losing Its Near Abroad," *Foreign Affairs*, July 24, 2025, https://www.foreignaffairs.com/russia/russia-losing-its-near-abroad-armenia-azerbaijan.

[35] Anton Troianovski, "Longtime Putin Aide Who Opposed Ukraine War Is Granted Rare Resignation," *The New York Times*, September 18, 2025, https://www.nytimes.com/2025/09/18/world/europe/russia-putin-kozak-resigns.html.

[36] "Putin izmenil strukturu upravleniya v administratsii prezidenta," *RBC*, August 29, 2025, https://www.rbc.ru/politics/29/08/2025/68b1e1cd9a7947a536ca8841.

[37] Alex Horobets, "Kozak's Departure Marks a Reset for Moscow's Post-Soviet Policy (Part Two)," *Eurasia Daily Monitor*, October 28, 2025, https://jamestown.org/kozaks-departure-marks-a-reset-for-moscows-post-soviet-policy-part-two/.

[38] Sergey Kanev, "Pancake," "Lenin," and an FSB hacker: Meet the fresh faces at Putin's new directorate "for strategic partnership and cooperation," *The Insider*, February 13, 2026, https://theins.press/en/inv/289376.

[39] Heads of SDA and Struktura, Ilya Gambashidze and Nikolai Tupikin, worked directly with Kiriyenko and his subordinate, Sofiya Zakharova. Their collective efforts resulted in the notorious Doppelgänger operation, which involved creating imitations of reputable Western media websites to disseminate disinformation. See: Hudson, John and Robyn Dixon, "Russian Disinformation Targets Ukrainian Leaders," *The Washington Post*, February 16, 2024, https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/; Jakob Hanke Vela, "FBI dossier reveals Putin's secret psychological warfare in Europe," *Politico*, September 5, 2024, https://www.politico.eu/article/fbi-dossier-reveals-russian-psy-ops-disinformation-campaign-election-europe/.

[40] "Ukraine's Intelligence: Russian Officials Suspected in Maidan-3 Destabilizing Campaign of Ukraine," *Kyiv Independent*, March 1, 2024, https://kyivindependent.com/ukraines-intelligence-russian-officials-suspects-in-ukraine-involved-in-maidan-3-destabilizing-campaign-of-ukraine/.

[41] Giorgi Menabde "Abkakhzia Expels Russian Political Technologists," *Jamestown Foundation*, April 12, 2025, https://jamestown.org/abkakhzia-expels-russian-political-technologists/; "The Kiriyenko Blueprint: Turning Moldova's Election Into an Operation," *Lansing Institute*, September 25, 2025, https://lansinginstitute.org/2025/09/25/the-kiriyenko-blueprint-turning-moldovas-election-into-an-operation/; Nerses Kopalyan, "Subversion and Electoral Interference: Russia and Armenia's 2026 Elections," *EVN Report*, April 2025, https://evnreport.com/evn-security-report/russia-and-armenias-2026-elections/.

[42] Andrey Pertsev, "Kirienko i nasledstvo Prigozhina v Afrike," *RIDL*, April 11, 2025, https://ridl.io/ru/kirienko-i-nasledstvo-prigozhina-v-afrike/.

[43] Kiriyenko has largely been seen as the curator of Russia's domestic policy bloc before extending his reach into foreign operations.

[44] While in theory tasked with overseeing domestic issues, other directorates under Kiriyenko's control, such as the ones for Social Projects, Domestic Policy as well Monitoring and Analysis of Social Processes have already been involved in foreign influence operations, such as the election interference in Armenia. See: Elena Mukhametshina, "Kuratrom otnoshenii s Armeniei v Administratsii Prezidenta stal Sergei Kirienko," *Vedomosti*, April 30, 2025, https://www.vedomosti.ru/politics/articles/2025/04/30/1107619-kuratorom-otnoshenii-s-armeniei-stal-kirienko.

[45] Mark Galeotti, *Prigozhin's Children* (Mayak Intelligence Ltd, 2024), 2, https://mayak-intelligence.com/wp-content/uploads/2024/10/report-prigozhins-children.pdf.
[46] Matt Murphy, "A year after mutiny, Kremlin controls Wagner remnants," *BBC*, June 23, 2024, https://www.bbc.com/news/articles/c4nn1p81q59o.
[47] Nicholas Chkhaidze, "PMC Redut: The Wagner Group's Potential Replacement," *Geopolitical Monitor*, August 30, 2023, https://www.geopoliticalmonitor.com/pmc-redut-the-wagner-groups-potential-replacement/.
[48] "How Russia's GRU Set Up a Fake Private Military Company for Its War in Ukraine," *Radio Free Europe/Radio Liberty*, October 10, 2023, https://www.svoboda.org/a/redut-schemes-systema/32630905.html.
[49] Bryjka, Filip and Jędrzej Czerep, *Africa Corps: A New Iteration of Russia's Old Military Presence in Africa* (Warsaw: Polish Institute of International Affairs, May 2024), 10, https://www.pism.pl/webroot/upload/files/Raport/PISM%20Report%20Africa%20Corps_.pdf; Ivan Klyshch, "Lyudi Rossi v Afrike," *Riddle*, July 1, 2024, https://ridl.io/ru/lyudi-rossii-v-afrike/.
[50] Anna Kruglova, "Russian Imperial Movement: The War in Ukraine and the Future of the Russian State," *ICCT*, September 1, 2023, https://icct.nl/publication/russian-imperial-movement-war-ukraine-and-future-russian-state; "Russian Imperial Movement: How a Far-Right Group Outlawed by the UK Is Spreading Terror Across Europe," *The Conversation*, July 14, 2025, https://theconversation.com/russian-imperial-movement-how-a-far-right-group-outlawed-by-the-uk-is-spreading-terror-across-europe-260825.
[51] Daniil Belovodyev, "Exclusive: The Russian Neo-Nazi Behind a Shadowy GRU Recruitment Campaign," *Radio Free Europe/Radio Liberty*, September 25, 2025, https://www.rferl.org/a/russia-gru-nazi-sabotage-recruitment-telegram/33539661.html.
[52] Richterova et al., "Russian Sabotage in the Gig-Economy Era."; Seth G. Jones, *Russia's Shadow War Against the West* (Washington, DC: Center for Strategic and International Studies, March 2025), 8, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250318_Jones_Russia_Shadow.pdf?VersionId=LHamL2L7HJwLgZ7a_wq6xkTIwMh3TFpk.
[53] Shaun Walker, "'These people are disposable': how Russia is using online recruits for a campaign of sabotage in Europe," *The Guardian*, May 4, 2025, https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe.
[54] Edwards, Charlie and Nate Seidenstein, *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*, Research Paper (The International Institute for Strategic Studies, 2025), 2, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf.
[55] Weiss, Michael, Roman Dobrokhotov, Christo Grozev, Fidelius Schmid, Nikolai Antoniadis, "Lost in translation: How Russia's new elite hit squad was compromised by an idiotic lapse in tradecraft," *The Insider*, Mar 13, 2026, https://theins.press/en/inv/290235.
[56] "GRU, terroristicheskie organizatsii i OPG," *Dossier Center*, https://gru.dossier.center/p2/crime/; Fatima Abo Alasrar, "The United States' Houthi terrorist designation unmasks Russia's Yemen strategy," *Atlantic Council*, March 14, 2025, https://www.atlanticcouncil.org/blogs/menasource/houthi-terrorist-designation-russias-yemen-strategy/.
[57] Michael Weiss, *Aquarium Leaks: Inside the GRU's Psychological Warfare Program* (Washington, DC: Free Russia Foundation, 2020), 8, https://think-tank.4freerussia.org/wp-content/uploads/2020/12/AquariumLeaks-EN-Web-1.pdf; *The GRU's Galaxy of Russian-Speaking Websites*, Report (Open Facto, January 2022), 3, https://drive.google.com/file/d/1xIbx6ZTy-BuQB_4iZ9JNureHJgHYu3Di0/view.
[58] *Analysis of the Russian Information Manipulation Set Storm-1516*, VIGINIUM Technical Report (SGDSN: May 7, 2025), 3, https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.
[59] "Useful idiots and their handlers. How the FSB's Fifth Service meddles in foreign states politics," *The Insider*, https://theins.press/en/investigations/useful-idiots-and-their-handlers-how-the-fsbs-fifth-service-meddles-in-foreign-states-politics; "FSB za granitsei," *Dossier Center*, https://fsb.dossier.center/abroad/.
[60] Jack Watling, "The Kaleidoscopic Campaigning of Russia's Special Services," *RUSI*, September 20, 2022, https://www.rusi.org/explore-our-research/publications/commentary/kaleidoscopic-campaigning-russias-special-services/.

[61] Watling, Danylyuk, and Reynolds, *Preliminary Lessons*, 4; Tkhorik, Vladimir, Sergey Kanev, Nicolae Kushkevich, and Marcela Zamosteanu, "Kuratory Moldovy s FSB," *RISE*, October 31, 2022, https://www.rise.md/rusa/%D0%BA%D1%83%D1%80%D0%B0%D1%82%D0%BE%D1%80%D1%8B-%D0%BC%D0%BE%D0%BB%D0%B4%D0%BE%D0%B2%D1%8B-%D0%B8%D0%B7-%D1%84%D1%81%D0%B1/; Dobrokhotov, Roman, Christo Grozev, and Michael Weiss, "Izmena po-ital'yanski. Kak Pyataya sluzhba FSB pokupala politikov iz Ligi Severa," *The Insider*, February 6, 2024, https://theins.press/inv/268904; Hugh Schofield, "French urged to watch out for Russian interference," *BBC*, November 7, 2023, https://www.bbc.com/news/world-europe-68414300; "The Insider: Propagandist Vladimir Sergienko Works for the Fifth Service of the FSB," *OCCRP*, February 5, 2024, https://www.occrp.org/ru/novosti/the-insider-propagandist-vladimir-sergienko-rabotaet-na-piatuiu-sluzbu-fsb.

[62] Grozev, Hristo, Roman Dobrokhotov, and Dada Lindell, "Chyorny piar. FSB nachala kampaniyu po dezinformatsii i konspirologii v Afrike," *The Insider*, February 8, 2024, https://theins.ru/inv/268965.

[63] Roman Anin, "Kak Putin prinyal reshenye o voyne," *iStories*, May 16, 2022, https://storage.googleapis.com/istories/opinions/2022/05/16/kak-putin-prinyal-reshenie-o-voine/index.html.

[64] Adam Jawor, "Managing consent: The FSB's Second Service and the full cycle of repression," *Defence24*, October 28, 2025, https://defence24.com/analysis-/managing-consent-the-fsbs-second-service-and-the-full-cycle-of-repression; "Sluzhba po zashchite konstitutsionnogo stroya i borbe s terrorizmom," *Dossier Center*, https://fsb.dossier.center/2s/; Dobrynin, Sergey, Mark Krutov, and Mike Eckel, "Vy chistye orki: kak agent FSB perepisyvalsya so svoimi kuratorami," *Radio Free Europe/Radio Liberty*, September 6, 2024, https://ww.svoboda.org/a/vy-chistye-orki-kak-agent-fsb-perepisyvalsya-so-svoimi-kuratorami/33108619.html.

[65] Jawor, "Managing Consent."

[66] "Report: FSB unit linked to Navalny poisoning now controls Russia's internet," *Meduza*, April 16, 2026, https://meduza.io/en/news/2026/04/16/report-fsb-unit-linked-to-navalny-poisoning-now-controls-russia-s-internet.

[67] "Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm," *U.S. Department of Justice*, July 9, 2024, https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners.

[68] Sergey Kanev, "Public-private espionage. How the GRU and FSB recruited a private company from Yekaterinburg to do their work around the world," *The Insider*, October 11, 2024, https://theins.ru/en/politics/275250; "Ukrainā sazīmēta krievu specdienestu darbinieka pēdas ved uz Latvijas un Lietuvas ostu biznesu," *TV3*, November 30, 2025, https://www.delfi.lv/bizness/19/bizness/120097170/ukraina-sazimeta-krievu-specdienestu-darbinieka-pedas-ved-uz-latvijas-un-lietuvas-ostu-biznesu.

[69] *Written evidence submitted by the Centre for Finance & Security at RUSI* (UK Parliament, March 2024), 1, https://committees.parliament.uk/writtenevidence/129260/pdf/.

[70] Andrey Pertsev, "The Bureau's niche project," *Meduza*, June 24, 2025, https://meduza.io/en/feature/2025/06/24/the-bureau-s-niche-project; "Neonatsistskaya gruppirovka "Rusich" budet okhranyat granitsu s Finlyandiyey," *Radio Free Europe/Radio Liberty*, September 9, 2024, https://www.severreal.org/a/neonatsistskaya-gruppirovka-rusich-budet-ohranyat-granitsu-s-finlyandiey/33113436.html.

[71] Mark Galeotti, *Gangsters at War: Russia's Use of Organized Crime as an Instrument of Statecraft*, Research Report (Geneva: Global Initiative Against Transnational Organized Crime, November 2024), 8, https://globalinitiative.net/wp-content/uploads/2024/10/Mark-Galeotti-Gangsters-at-war-Russias-use-of-organized-crime-as-an-instrument-of-statecraft-GI-TOC-November-2024.pdf.

[72] Mark Galeotti, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, Policy Brief (European Council on Foreign Relations, April 2017), 6, https://ecfr.eu/wp-content/uploads/ECFR208_-_CRIMINTERM_-_HOW_RUSSIAN_ORGANISED_CRIME_OPERATES_IN_EUROPE02.pdf.

[73] "FSB's Magnificent Seven: New Links Between Berlin and Istanbul Assassinations," *Bellingcat*, June 29, 2020, https://www.bellingcat.com/news/europe/2020/06/29/fsbs-magnificent-seven-new-links-between-berlin-and-istanbul-assassinations/.

[74] Working through NGOs, GONGOs, and think tanks is not exclusive to the SVR, as the GRU and FSB are also known to leverage such proxies. For example, FSB is known to have ties with the Institute of CIS Countries, while GRU – with the Institute of the Russian Diaspora. In many cases, multiple RISS can be linked to the same proxies. See: *Russian Think Tanks Promote Kremlin Interests in the West* (Tallin: EFIS, December 20, 2024), https://raport.valisluureamet.ee/2025/en/3-russian-foreign-policy/3-4-russian-think-tanks-promote-kremlin-interests-in-the-west/; Soldatov, Andrei and Michael Weiss, "Inside Russia's Secret Propaganda Unit," *New Lines Magazine*, December 7, 2020, https://newlinesmag.com/reportage/inside-russias-secret-propaganda-unit/.

[75] Grzegorz G. Rzeczkowski, "Służba Putina do zadań specjalnych zatruwa Polskę. Tak działa RISI," *Gazeta Wyborcza*, April 20, 2022, https://wyborcza.pl/7,75398,28351668,sluzba-putina-do-zadan-specjalnych-zatruwa-polske-tak-dziala.html.
[76] Andrew Roth, "Revealed: Russian legal foundation linked to Kremlin activities in Europe," *The Guardian*, June 2, 2024, https://www.theguardian.com/world/article/2024/jun/02/revealed-russian-legal-defence-foundation-pravfond-europe.
[77] "Chto takoe i zachem nuzhno Rossotrudnichestvo," *Dossier Center*, February 24, 2021, https://dossier.center/rossotr/; Linda Hourani, "Hiding in plain sight – how Russia's cultural centers continue to operate in US, Europe despite espionage claims," *Kyiv Independent*, June 4, 2025, https://kyivindependent.com/cultural-diplomacy-or-cover-for-espionage-why-russian-cultural-centers-remain-open-across-the-globe/.
[78] Sergey Kanev, "Kukla v pogonakh. Vmesto vyslannykh iz Avstrii shpionov, rabotavshikh pod prikrytiem TASS, Kreml prislal novykh," *The Insider*, October 2, 2025, https://theins.ru/inv/285463.
[79] During the Cold War, it was common practice for KGB officers to be embedded within the international news teams of TASS in order to gain access to foreign journalistic circles. See: *TASS: Its Role, Structure and Operations* (Central Intelligence Agency, 1959), 24, www.cia.gov/readingroom/docs/CIA-RDP78-02771R000100330004-8.pdf; Jacques Follorou, "When the KGB Took an Interest in *Le Monde*," *Le Monde*, January 6, 2025, https://www.lemonde.fr/en/history/article/2025/01/06/when-the-kgb-took-an-interest-in-le-monde_6736763_157.html; Kanev, "Spies, Banquets, and Embezzlement."
[80] "Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors," *U.S. Department of the Treasury*, March 3, 2022, https://home.treasury.gov/news/press-releases/jy0628.
[81] Weiss, Michael, Roman Dobrokhotov, Christo Grozev, "Morality and ethics should play no part: Leaks reveal how Russia's foreign intelligence agency runs disinformation campaigns in the West," *The Insider*, July 4, 2024, https://theins.press/en/politics/272870.
[82] Layan, Eloïse, Léa Peruchon, Sofía Álvarez Jurado, "Sixty Russian agents identified: Prigozhin's influence network taken over by the Foreign Intelligence Service," *Forbidden Stories*, 20 February 2026, https://forbiddenstories.org/russian-agents-prigozhins-influence-network-taken-over-by-the-intelligence-service/.
[83] Dina Temple-Raston, "A Worst Nightmare Cyberattack: The Untold Story of the SolarWinds Hack," *NPR*, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack; Weiss, Dobrokhotov, Grozev, "Morality and ethics should play no part."
[84] Galeotti Mark, *Putin's Praetorians: The Evolving Role of the National Guard and Their Capacity to Control the Streets* (Mayak Intelligence Ltd, 2024), 4, https://mayak-intelligence.com/wp-content/uploads/2024/09/report-putins-praetorians.pdf; Igor Torbakov, "The Praetorian Guard of Putin Must Quell Internal Unrest," *Platform RAAM*, September 21, 2017, https://platform-raam.nl/artikelen/709-the-praetorian-guard-of-putin-must-quell-internal-unrest.
[85] Lorenzo Crippa, "Putin's Henchmen: The Russian National Guard in the Invasion of Ukraine," *International Centre for Defence and Security*, https://icds.ee/en/putins-henchmen-the-russian-national-guard-in-the-invasion-of-ukraine/4.
[86] Jolanta Darczewska, *Putin's Cossacks: Folklore, Business or Politics?* (Warsaw: Centre for Eastern Studies, December 2017), 8, https://www.osw.waw.pl/sites/default/files/pw_68_putin_cossacks_net_0.pdf; "Peskov: kazakov vklyuchat v sostav Rosgvardii," *Kommersant*, July 13, 2021, https://www.kommersant.ru/doc/4899351.
[87] Richard Arnold, "Russia's Cossack Movement Holds Second Great Circle in Two Years," *Eurasia Daily Monitor*, April 17, 2025, https://jamestown.org/russias-cossack-movement-holds-second-great-circle-in-two-years/.
[88] *Ibid*.
[89] Laura Linderman and Anna Harvey, *Kadyrov's Chechnya: The State Within Putin's State* (Central Asia-Caucasus Institute & Silk Road Studies Program Joint Ceter, 2016), 2, https://www.cacianalyst.org/resources/Kadyrovs_Chechnya_The_State_Within_Putins_State_final.pdf.
[90] "Russia Deploys Occupation Enforcers Close to Ukraine," *CEPA*, February 8, 2022, https://cepa.org/article/russia-deploys-occupation-enforcers-close-to-ukraine/.
[91] Kimberly Marten, "Where's Wagner Now? One Year after the Mutiny," *PONARS Eurasia*, June 21, 2024, https://www.ponarseurasia.org/wheres-wagner-now-one-year-after-the-mutiny/.
[92] "Pavel Prigozhin vozglavil podrazdelenie Rosgvardii, kuda voshla ChVK Vagner," *Kommersant*, November 1, 2023, https://www.kommersant.ru/doc/6312235.

Reflexive Control in Financial Markets

Detecting Doctrinal Influence Operations in the Cognitive Battlespace of Global Finance

By James Tennant and Andrew MacKay

Introduction

Allied nations have invested heavily in offensive financial warfare capabilities, particularly since 2001, while leaving the cognitive integrity of their own markets essentially undefended. This article argues that reflexive control, a Soviet-origin military doctrine formalised by Lefebvre (1967) and operationalised by Komov (1997), is being applied to financial markets with alarming precision.[1] Six observable signatures derived from the doctrinal literature are identified: predetermined decision framing, false certainty about hidden information, reflexive trap structure, narrative laundering of state-media content, timing coincidence, and network anomaly. A companion empirical study covering ten sanctions events between 2022 and 2024, using standard event study methodology (MacKinlay, 1997) with cross-sectional significance testing, finds significant abnormal returns and volume concentrated in directly affected securities, consistent with targeted narrative shaping.[2] The article argues this is an irregular warfare problem, not a securities regulation problem, and proposes four institutional responses: doctrinal surveillance layers on

James Tennant is a doctoral candidate at the University of Technology Sydney, where his research examines how liberal democracies should conceptualise, operationalise, and institutionalise economic and financial warfare as a strategic instrument. He is a Partner at BOKA Capital, a Fellow at the Australian Strategic Policy Institute's Cyber, Technology and Security Programme, and a Captain in the Australian Army. His professional work spans defence, intelligence, and financial services.

Andrew Mackay is a former British Naval officer and defence strategist specializing in Threat Finance and Economic Levers, with extensive experience in irregular warfare, hybrid threats, and strategic communications. He has served in Bosnia, Iraq, Afghanistan and Bahrain, across NATO and in Washington DC. He is a former country head of financial crime threat mitigation with a global bank and is an Associate Fellow at RUSI Centre for Finance and Security (CFS) and a PhD candidate at the United Nations University.

market data feeds, convergent evidence standards, a shared allied narrative monitoring capability, and explicit defensive doctrine for financial market integrity.

The Blind Spot

On 28 February 2022, *British Petroleum* (*BP*) announced it would walk away from its 19.75 percent stake in Rosneft.[3] Within three trading days, *BP*'s London-listed shares dropped on the order of six percent.[4] Within a week, they recovered by roughly seven percent. The initial sell-off shows a pattern consistent with a narrative-driven overreaction rather than a pure fundamentals response: prices moved sharply amid a wave of breathless commentary across trading forums and social media, then partially reversed as more measured analysis emerged. That kind of overreaction-reversal pattern is well documented in behavioral finance as a feature of narrative-driven trading, where stories can move prices faster than updated fundamentals. Two weeks later, Washington banned Russian oil imports. In the five days before the formal announcement, ExxonMobil's shares climbed to the order of ten percent. The ban was telegraphed through policy statements, media leaks, and a surge of social media posts that framed the outcome as inevitable and pointed to a single obvious trade. By the time the announcement hit, the trade was already crowded.[5] Then came the reversal: a sharp decline of around fifteen percent as the market digested reality rather than narrative.[6] Someone made money on that volatility. The question is who, and whether the narrative shaping was organic or orchestrated.

These are not isolated oddities. A companion empirical study has examined ten sanctions events between 2022 and 2024 using standard market model event study methods (MacKinlay, 1997), with cross-sectional significance testing (Boehmer, Musumeci, and Poulsen, 1991) and volume analysis over three-day and five-day event windows.[7] The pattern holds: where firm-specific exposure to sanctions is highest, abnormal returns and abnormal trading volume concentrate[8]. Volume spikes where price spikes, and both cluster around the events where the information environment was most actively shaped. The eight events with lower firm-specific exposure show noise, not signal. This concentration pattern matters because it is consistent with targeted narrative operations rather than generalized market stress.

But what does "the information environment was actively shaped" actually mean? Who is doing the shaping, using what techniques, and how would we know? That is the question this article addresses. It argues that a specific family of psychological techniques, formalized in Russian military doctrine under the name *reflexive control*, maps onto financial markets with alarming precision. These techniques have a sixty-year doctrinal pedigree, a proven track record in military and political operations, and a set of observable signatures that can be detected computationally. And the current infrastructure for monitoring market integrity is largely blind to them, or at best only incidentally sensitive to them.

A Doctrine Designed for Exactly This

Reflexive control is not a metaphor or an analogy. It is a formalized military doctrine with roots in Soviet-era decision science. Lefebvre laid the theoretical foundations in 1967, describing how one actor transmits a carefully constructed information package to an adversary such that the adversary voluntarily arrives at a decision predetermined by the sender.[9] Komov operationalized the theory for the Russian General Staff in 1997, specifying eight methods including distraction, overload, paralysis, deception, and intimidation, each designed to constrain the adversary's perceived option space.[10] Snegovaya documented its application in the infor-

mation campaigns observed during the Ukraine conflict from 2014 onwards.[11]

The word *voluntarily* is doing the heavy lifting in Lefebvre's definition. The target does not feel coerced. The information package is designed so the "correct" conclusion appears to emerge from the target's own reasoning. The adversary believes the decision is theirs. It is not. This is what separates reflexive control from crude propaganda or disinformation. Propaganda tries to change what you believe. Disinformation tries to make you believe something false. Reflexive control does not. It accepts what you already believe and restructures the framing so that your own reasoning leads you to a predetermined action. The underlying facts might be entirely accurate. The manipulation is in the architecture of the choice.

This distinction has practical consequences for countermeasures. Western democracies have built substantial infrastructure for countering disinformation: fact-checking organizations, platform content moderation policies, media literacy campaigns, and government-backed counter-narratives. These tools are designed for a world where the threat is false information. Reflexive control sidesteps all of them. A fact-checker cannot flag a post that contains no false statements. A content moderation algorithm trained on misinformation markers will not trigger on a post that uses accurate information in a coercive frame. A media literacy program that teaches people to verify facts will not help if the facts are real and only the framing is adversarial.[12] The entire Western counter-disinformation apparatus is optimized as a threat model that reflexive control does not fit.[13]

On a battlefield, the target is a commander, and the predetermined decision might be to reinforce the wrong sector or hold fire when aggression is the better option. In a financial market, the target is a trader, a portfolio manager, or a retail investor scrolling *Reddit* at midnight, and the predetermined decision is a specific trading action. A social media post that says "the only rational move is to sell before the freeze" is not offering analysis. It is closing the decision space to a single action that serves someone else's position.

This matters enormously for detection. Market surveillance systems at exchanges, compliance teams, and financial regulators are built to catch profit-seeking fraud: insider trading, front-running, pump-and-dump schemes.[14] They look for someone to make money illegally. But a reflexive control campaign run by a state-linked actor is not trying to make money. It is trying to move a price, erode confidence, or create chaos in a specific sector at a strategically useful moment. It does not need to generate a trading profit to succeed. It does not need to make false statements. Existing surveillance infrastructure is poorly equipped to catch it because it is tuned to different motives and methods.

Thomas provided the English-language intelligence community's most detailed assessment of how the doctrine works in military practice.[15] Giles traced the institutional pipeline from Cold War military science to contemporary information operations.[16] Rid documented the broader lineage of active measures across decades of Soviet and Russian operations.[17] Pomerantsev gave it human texture, describing the working culture inside the organizations that develop and deploy these techniques.[18] Shiller's work on narrative economics established that stories, not just data, drive market behavior, providing the theoretical mechanism through which reflexive control techniques gain traction among investors.[19] But none of these authors looked at financial markets as a target set. The finance literature, for its part, has modelled social media manipulation extensively but treats it as profit-motivated retail behavior. Nobody has stood between the two literatures and asked the obvious question: what happens when a state actor points military-grade psychological doctrine at civilian

investors who have no training, no intelligence support, and no institutional defense?

The vulnerability is structural. Retail investors process information through platforms designed to reward engagement over accuracy.[20] Commission-free trading apps have put consequential financial decisions in the hands of millions of people who consume their market information through the same social media channels that state-linked influence operations use for targeting. The attack surface is enormous, and it is growing. These are precisely the conditions under which reflexive control is most effective: time pressure, incomplete information, a large and untrained target population, and delivery channels that the target trusts.[21]

What It Looks Like in a Trading Feed

If you know what the doctrine prescribes, you can recognize its signatures in the wild. The research program behind this article identified six patterns that map directly to elements of the Lefebvre-Komov tradition and that can be detected through automated analysis of social media text. Each one corresponds to something a trained analyst can spot in a *Reddit* thread, a T*elegram* channel, or a finance-focused *X* account.

The most obvious is *predetermined decision framing*: language that eliminates alternatives. Not "I think the stock will fall" but "the only rational move is to sell immediately." The difference is operationally significant. The first is an opinion that invites disagreement. The second restructures the reader's perceived option space so that only one action appears available. In a busy trading feed where people are making fast decisions under stress, that framing is powerful.

The second pattern is *false certainty about hidden information*: claims like "the desk is dumping" or "my sources confirm the block trade is coming." The poster asserts privileged access to information the reader cannot verify, creating an artificial asymmetry that pressures the reader toward the predetermined action. In Komov's terminology, this is deception layered with cognitive overload: give the target too much to process and a simple conclusion to fall back on.

Third is the *reflexive trap*: a post that starts with something the reader already believes ("the Fed raised rates"), chains through plausible-sounding inferences ("banks will tighten lending, which will hit real estate, which will crush construction stocks"), and arrives at a specific directive ("get out of XYZ before Friday"). Each step is individually reasonable. The manipulation is in presenting the chain as inevitable and the conclusion as the only available action. This is the full Lefebvre loop executed in a single social media post.

The fourth, *narrative laundering*, is the bridge between the information warfare world and the financial world. A post on a retail investing forum about oil futures uses the same framing, vocabulary, and causal logic as an *RT* or *TASS* article published hours earlier but presents it as the poster's own independent analysis. The content has been laundered from a state-media channel into a retail trading context. Detection works by measuring textual overlap between social media posts and a reference corpus of state-media output drawn from the Global Database of Events, Language, and Tone (GDELT) archive.[22] When the overlap is high and the posting account is young, the convergence is telling.

The remaining two patterns are structural rather than textual. *Timing coincidence* flags accounts that appear or activate within a narrow window before a market-moving event, suggesting pre-positioning rather than organic participation. An account created three days before a sanctions announcement that immediately begins posting about the affected securities warrants a different kind of scrutiny than the same content from a five-year-old account with a long posting history.[23] *Network anomaly* flags clusters of accounts that post

in synchronized bursts, share linguistic fingerprints, or amplify each other in ways that real communities do not.[24] When two or more of these six patterns converge in the same post or cluster of posts, the combined signal is the detection trigger.[25]

Inside an Event: The BP-Rosneft Information Environment

Theory is useful, but practitioners need operational texture. Consider what the information environment around *the BP-Rosneft* event looked like.

In the 48 hours before *BP*'s announcement on February 28, 2022, social media activity on finance-focused *Reddit* communities and *Telegram* channels showed a detectable shift. Posts about *BP* and *Rosneft* increased sharply, which is expected when a major geopolitical event is unfolding. What was less expected was the character of the posts. A significant cluster did not simply discuss the news. They framed a single trading conclusion as inevitable: that *BP* would be forced to divest, that the share price would collapse, and that anyone still holding was being reckless. The language was not analytical. It was directive. "Get out before Monday" appeared in multiple variations across accounts with limited posting histories.

At the same time, the *GDELT* state-media corpus showed a parallel surge. *RT* and *TASS*[26] articles published on February 26 and 27, 2022, framed the Western sanctions response as panicked, economically self-destructive, and evidence of a broader Western decline. The causal framing in these articles, specifically that sanctions would hurt Western companies more than Russia, appeared in paraphrased form across retail trading forums within hours. The content had been laundered: same framing, same causal logic, different voice. Individual posts looked like organic retail commentary. In aggregate, the overlap with state-media talking points was measurable.

The timing pattern added context. Several of the accounts driving the most directive language had been created in the preceding two weeks. They had minimal prior activity. They posted about the affected securities, made strong directional claims, and then went quiet. This is not proof of a state-directed operation. It is, however, a pattern that is operationally consistent with coordinated inauthentic deployment, and it is a pattern that current market surveillance tools are not configured to detect.

The market response followed the narrative. *BP* shares fell nearly six percent in three days, overshooting what the fundamental impact of the divestiture alone would justify. Trading volume more than doubled relative to the estimation-window average. Then came the correction: a seven percent bounce as institutional analysts published their own assessments and the panic subsided. The overreaction-reversal pattern is exactly what you would expect if narrative shaping had temporarily displaced fundamental analysis in driving trading decisions.

Beyond Russia: The Chinese Dimension

The doctrinal analysis so far has focused on the Russian tradition because it is the most formalized and the best documented in English-language sources. But reflexive control is not the only state-level doctrine for shaping adversary decision-making through information. China's "Three Warfares" concept, formally adopted by the Central Military Commission in 2003, provides a parallel framework that is at least as relevant to financial markets and arguably more dangerous in the long term.[27]

The "Three Warfares" -- public opinion warfare, psychological warfare, and legal warfare -- operate differently from the Russian model. Where Russian reflexive control tends to be tactical and opportunistic, exploiting specific events through rapid deployment of narrative assets, the Chinese approach is institutional and patient. Public opinion warfare shapes the broader information environment over months and years, building narratives about economic inevitability (the "rise of China"

frame) that create a pre-existing cognitive landscape favorable to specific trading decisions. Psychological warfare targets the confidence of specific actors: fund managers considering China exposure, corporate boards evaluating supply chain decisions, sovereign wealth funds assessing geopolitical risk. Legal warfare uses regulatory and legal instruments to create market conditions that channel capital in desired directions.[28]

Applied to financial markets, this means the detection challenge is different. Russian-style reflexive control shows up as a burst of activity around a specific event. Chinese-style narrative warfare shows up as a slow shift in the baseline assumptions that market participants bring to their decisions. Both manipulate the decision environment. But the Russian version can be detected by looking for anomalous spikes. The Chinese version requires monitoring drift in baseline narratives over time, which is a fundamentally harder detection problem and one that existing surveillance infrastructure is even less equipped to handle.

A comprehensive allied detection capability will need to address both. The six patterns described in this article are calibrated for the Russian model. Extending them to Chinese "Three Warfares" techniques would require additional features: tracking the gradual alignment of retail trading narratives with state-media themes over weeks rather than hours, monitoring the sentiment trajectory of discussions about China-exposed sectors, and detecting legal warfare signals such as the strategic timing of regulatory announcements designed to move specific markets. This is a research frontier, not a solved problem, but it is a frontier that the irregular warfare community cannot afford to ignore.

Concrete examples illustrate the operational difference. During the 2020-2021 regulatory crackdown on Chinese technology companies, Western institutional investors lost significant value as *Ant Group*'s IPO was suspended and *Didi Global* was forced to delist from the New York Stock Exchange.[29] The information environment around these events was preceded by state-media narratives that framed foreign listings as a national security vulnerability, creating a context in which regulatory intervention could plausibly be anticipated even if its timing and scope were unclear. This is not the rapid, event-triggered pattern of Russian reflexive control. It is the slow construction of a cognitive baseline that makes a specific market outcome feel inevitable when it arrives. Detecting this requires tools that measure narrative drift over weeks and months, tracking the gradual alignment of state-media themes with shifts in investor sentiment toward China-exposed sectors. The challenge is compounded by the scale and sophistication of China's state-media apparatus, which operates across multiple languages and platforms with a coordination capacity that dwarfs the Russian model.

Why This Is an Irregular Warfare Problem; Not a Regulatory One

The framing question matters more than the detection question. Whether reflexive control in financial markets is treated as a securities regulation problem or a national security problem determines everything that follows--which agencies lead, which legal authorities apply, which budgets are allocated, and which allied partners are brought in.

If it is a regulation problem, the response sits with the Australian Securities and Investments Commission (ASIC) in Australia, the Financial Conduct Authority (FCA) in the United Kingdom, or the Securities and Exchange Commission (SEC) in the United States. They will look for market manipulation under existing securities law, which requires demonstrating intent to deceive for profit. A state-linked operation that shapes market narratives for geopolitical advantage, using accurate information selectively framed, will fall outside this framework entirely. No false statement of fact means no basis for

enforcement. No identifiable profit motive means no fraud case. No insider relationship means no insider trading charge. Every element of the standard regulatory toolkit requires something that a well-designed reflexive control operation deliberately avoids providing. The regulator has the wrong map.

If it is a national security problem, the response sits at the intersection of financial intelligence and signals intelligence. The legal authorities shift. The detection infrastructure shifts from trade surveillance to narrative monitoring. The allied coordination shifts from regulatory mutual assistance to intelligence sharing. These are not minor bureaucratic distinctions. They are fundamentally different institutional architectures producing fundamentally different capabilities.

The evidence supports the national security framing. The companion event study finds market effects around sanctions announcements, which are state actions. The detection features are derived from military doctrine, not from securities fraud typologies. The narrative laundering pattern explicitly traces content from state media into retail trading channels. This is not simply market manipulation with geopolitical flavor. It is more accurately understood as an irregular warfare problem that uses financial markets as its medium.

An important caveat applies to any claims drawn from this evidence. The market patterns observed are consistent with reflexive control operations, but consistency is not the same as attribution. Abnormal returns around geopolitically charged events can arise from organic investor behavior, herding, algorithmic amplification, or legitimate anticipatory trading by well-informed market participants. The presence of doctrinal signatures in social media text does not prove state direction; it proves that the techniques described in the doctrine are present in the information environment. Moving from "consistent with" to "attributable to" requires convergent evidence from multiple independent sources, including classified intelligence that this research does not access. The framework presented here is designed to flag candidates for further investigation, not to deliver definitive attribution on its own.

Valery Gerasimov's 2013 article, often characterized as a blueprint for hybrid warfare though some scholars argue it is better read as a description of Western methods observed by the Russian General Staff, recognized the blurring of military and non-military instruments, including economic measures, into a single operational continuum.[30] Financial markets sit squarely within that continuum. The infrastructure that enables global capital flows, Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging, correspondent banking, central securities depositories, and derivatives clearing houses, constitutes systemically important financial infrastructure that, while not owned by any single nation (SWIFT itself is a Belgian cooperative), functions as a critical enabler of global economic activity. An adversary who can manipulate the information environment around these systems achieves strategic effects without breaching a network or firing a weapon.

The concept of an economic kill chain, analogous to *Lockheed Martin*'s cyber kill chain but adapted for financial warfare, provides the operational sequencing.[31] A financial warfare campaign moves through reconnaissance, mapping of chokepoints, positioning, execution, amplification, exploitation, and assessment.[32] Reflexive control maps to the execution and amplification phases: the psychological operations component that shapes market behavior to complement the structural pressure of sanctions, asset freezes, and market access denial.[33] Understanding this sequencing reframes the detection problem. It is not about finding a single bad post. It is about recognizing a campaign.

Consider how this plays out institutionally. A surge of social media posts appears across *Reddit*

and *Telegram* in the hours before a major sanctions announcement. The posts use language that narrows the reader's options to a single trade. Some of them track closely with *RT* and *TASS* articles published earlier that day. The posting accounts are young. Who notices? The exchange's market surveillance team is watching for spoofing and layering. The compliance department is monitoring for insider trading. The financial regulator is looking for materially misleading statements. None of them are looking for doctrinal signatures in the text of social media posts. The intelligence community, which might recognize the pattern, typically does not monitor retail trading forums as part of its routine remit. The information tends to fall into a gap between institutions, and the gap is where the adversary operates.

This institutional gap is not a design flaw in any single agency. It is an artefact of how the problem has been categorized. Securities regulation and national security were built as separate institutional architectures because the threats they addressed were assumed to be distinct. Profit-seeking fraud goes to the regulator. State-directed operations go to the intelligence community. Reflexive control in financial markets sits in the overlap, and no agency is clearly mandated to own that overlap. Until one does, or until a coordination mechanism bridges them, the adversary has a free run.

What the Cyber Transition Teaches Us

Financial narrative defense is not the first domain to face this institutional categorization problem. Cybersecurity went through an almost identical transition, and the parallels are instructive.

For most of the 1990s and early 2000s, cybersecurity was treated as an IT problem. It sat with chief information officers and network administrators. The institutional assumption was that cyber threats were technical, that they targeted systems rather than strategic interests, and that the response belonged in the technology function rather than the national security apparatus. It took a series of escalating incidents to shift that assumption.[34] The U.S. Office of Personnel Management (OPM) breach in 2015 demonstrated that a state actor could steal the personal records of 22 million government employees through a cyber intrusion. *SolarWinds* in 2020 showed that a supply chain compromise could give a foreign intelligence service persistent access to government agencies. *Colonial Pipeline* in 2021 demonstrated that a ransomware attack on a single company could disrupt fuel supply across the eastern United States.

Each incident moved the institutional needle. After OPM, the U.S. government created the Cybersecurity and Infrastructure Security Agency (CISA). After *SolarWinds*, the White House issued an executive order on improving national cybersecurity. After *Colonial Pipeline*, the U.S. Transportation Security Administration (TSA) imposed mandatory cybersecurity requirements on pipeline operators.[35] The pattern is clear: institutional reform followed catastrophic failure, not foresight.

Financial narrative defense is at the start of that same curve. The threat is real, the evidence is accumulating, and the institutional response is absent. The question is whether allied nations will learn from the cyber precedent and build capability before a catastrophic incident forces them to, or whether they will wait until a financial equivalent of *Colonial Pipeline* exposes the gap: a state-directed narrative campaign that moves a major market, damages civilian investors, and leaves policymakers scrambling to explain why nobody was watching. The institutional tools that emerged from the cyber transition, threat sharing alliances, mandatory incident reporting, critical infrastructure designations, sector-specific agencies, all have financial narrative analogues. The design patterns exist. The political will to apply them does not, yet.

What Allied Nations Should Do About It

Four things need to happen, and they need to happen across agencies rather than within them.

The first is the simplest and the most overdue: *layer doctrinal recognition onto existing market surveillance.* Exchanges and regulators already monitor trading feeds for anomalous patterns. What they do not monitor for is doctrinal signatures: the specific linguistic and behavioral patterns that distinguish a state-linked influence operation from organic market commentary. The six patterns described in this article, and potentially others drawn from Chinese "Three Warfares" doctrine and Western military deception (MILDEC) traditions, can be integrated into existing surveillance infrastructure without replacing it. The gap is not technological. It is conceptual. Nobody has asked the surveillance systems to look for military doctrine because nobody in the regulatory chain has framed the problem that way. Practically, this means adding a doctrinal analysis module to the natural language processing tools that surveillance teams already use. The detection patterns are rule-based and interpretable; they do not require exotic technology. What they require is a decision by someone in the regulatory or intelligence chain to deploy them.

The second is to *establish convergent evidence standards for detection claims.* The intelligence community and the academic community do not trust each other's methods, for understandable reasons. Intelligence assessments rely on classified sources that cannot be disclosed. Academic research demands reproducibility and statistical rigor but rarely has access to classified material. The approach used in the companion study, pairing content analysis with an independent event study that shares no data with the classifier, produces evidence that satisfies both: analytical tradecraft for the intelligence consumer, statistical robustness for the academic reviewer, and a dual evidence chain strong enough for legal proceedings. Allied nations building detection capability should adopt this kind of convergent design as standard operating procedure. The alternative is a situation where intelligence agencies make claims about adversary financial operations that cannot be independently verified, which invites both politicization and dismissal.

The third is to *build a shared allied capability for monitoring financial narrative campaigns. The* reference corpus of state-media output used in this research is publicly available through *GDELT*. But real-time detection of narrative laundering across platforms requires social media data feeds, platform application programming interfaces (APIs), and cross-language processing at a scale that individual agencies cannot sustain. A shared allied capability, modelled on structures like the *Cyber Threat Alliance*, would turn retrospective research into operational early warning.[36] The technical infrastructure for this kind of monitoring exists in other intelligence domains. The gap is institutional, not technological, and closing it requires political will more than funding. The model already exists in cyber threat intelligence: allied nations share indicators of compromise, threat actor profiles, and attack methodologies through established channels. Financial narrative threats are structurally similar. The indicators are textual and behavioral rather than technical, but the sharing architecture is the same. What is missing is the decision to extend the existing framework to cover this domain.

The fourth, and the one that will take the longest, is to *develop explicit defensive doctrine for financial market integrity.* Australia, the United Kingdom, and the United States each maintain sophisticated offensive financial warfare capabilities. The offensive playbook is comparatively mature: asset freezes, correspondent banking restrictions, secondary sanctions, sovereign debt exclusions. Defensive doctrine, the concepts, procedures, and

institutional arrangements for protecting domestic markets from adversary narrative operations, is far less developed. What would it include? Real-time monitoring infrastructure. Analyst training in doctrinal recognition. Legal authorities for intervention when state-linked manipulation is identified. Coordination protocols between financial regulators, intelligence agencies, and allied partners. Information-sharing agreements covering financial narrative threats alongside existing cyber and counterterrorism cooperation.

The Legal Authority Gap

Institutional will is necessary but not sufficient. The legal frameworks also need examination, because the current authorities were not designed for this threat.

In Australia, the Security of Critical Infrastructure Act 2018, as amended in 2022, designates certain financial market infrastructure as critical infrastructure and empowers the government to impose positive security obligations and, in extreme cases, direct action.[37] The Act's definition of a "cyber security incident" has been framed with technical and operational disruptions in mind. Whether, and how, it should be extended to cover information operations that degrade the integrity of financial market data feeds would be a policy choice, likely requiring explicit regulatory or legislative clarification. The Act was written with cyber and physical threats in mind, not narrative operations. Extending it would require acknowledging that the information environment around critical infrastructure is itself part of the infrastructure.

In the United States, the International Emergency Economic Powers Act (IEEPA) provides broad presidential authority to regulate economic transactions in response to unusual and extraordinary threats.[38] IEEPA has been used to impose sanctions, freeze assets, and restrict trade. Whether it could be used to authorize defensive measures against narrative operations targeting financial markets is an open legal question, but the statutory language is broad. Any such use would raise novel issues that have not yet been tested in practice. The more immediate gap is at the regulatory level: neither the SEC nor Commodities Futures Trading Commission (CFTC) has a mandate or a mechanism for addressing market manipulation that serves geopolitical rather than profit-seeking objectives.

In the United Kingdom, the National Security Act 2023 creates offences related to foreign interference, including conduct intended to influence a political, economic, or other process. Whether a state-directed narrative campaign targeting the London Stock Exchange would fall within the scope of "foreign interference" is a question that has not been tested. The FCA's market abuse powers require demonstrating a false or misleading impression, which a reflexive control campaign using accurate information would not trigger.[39]

Across all three jurisdictions, the pattern is the same: the legal authorities were designed for threats that the legislators of the time understood. Cyber threats prompted cyber legislation. Terrorism prompted terrorism legislation. Financial narrative warfare has not yet prompted its own legislative response because the threat has not yet produced a sufficiently visible failure. The irregular warfare community should be making the case for pre-emptive legislative action rather than waiting for the incident that forces it.

Any monitoring capability of the kind described here raises significant civil liberties questions that this article does not attempt to resolve but must acknowledge. In the United States, First Amendment protections place substantial constraints on government monitoring of speech, even speech that serves an adversary's strategic objectives. The European Convention on Human Rights, particularly Article 10 on freedom of expression and

Article 8 on privacy, imposes similar constraints across European jurisdictions. In Australia, while constitutional free speech protections are more limited, the implied freedom of political communication and the Privacy Act 1988 create a legal environment in which surveillance of social media for doctrinal content would require careful legislative design to avoid overreach. The tension is real: a monitoring capability powerful enough to detect state-linked narrative campaigns is also powerful enough to chill legitimate political speech, market commentary, and financial journalism. Institutional safeguards, including judicial oversight, warrant requirements for identifying individual users, strict data minimization protocols, and independent review mechanisms, would be necessary but not sufficient to address the civil liberties risks. They would need to be built into any operational framework from the outset, not retrofitted after a civil liberties challenge forces the issue.[40]

What that legislative reform should target is relatively clear. The core problem is definitional. Existing market abuse statutes define manipulation in terms of intent to profit or to create false impressions. A reflexive control campaign does neither in the conventional sense. It uses accurate information, selectively amplified, to produce a decision environment that serves geopolitical rather than commercial objectives. Legislators need to create a category of foreign state-directed market interference that is distinct from conventional market manipulation and that does not require proof of profit-seeking intent. The threshold for intervention should be tied to the convergence of doctrinal signatures rather than to the content of any individual communication. This is analogous to the way counter-terrorism legislation shifted from criminalizing specific acts to criminalizing preparatory conduct that demonstrated coordinated hostile intent. The financial domain needs an equivalent conceptual shift, and the IW community is better placed than financial regulators to articulate what that shift should look like.

What the Capability Actually Looks Like

Policy recommendations are easy to write and hard to implement. What would an operational financial narrative monitoring capability actually look like in practice?

Start with the monitoring floor. A joint cell, ideally hosted within an existing intelligence fusion center, staffed by analysts drawn from financial regulators, signals intelligence agencies, and open-source intelligence units. The cell ingests three data feeds in real time: social media from finance-relevant platforms (*Reddit*, *Telegram*, *X*, *StockTwits*, and their non-English equivalents), state-media output from *GDELT* and equivalent sources, and market data including price, volume, and order flow from the exchanges themselves. The detection pipeline runs automated screening against the six doctrinal patterns described in this article, flagging content for human review when two or more patterns converge.

Human analysts provide the second layer. Automated detection catches the signature; human judgement determines whether the signature reflects a genuine campaign or a false positive. The analyst asks: does this cluster of flagged content align with a known geopolitical trigger? Is there a sanctions event, a military escalation, or a diplomatic crisis that would provide the strategic context for a reflexive control operation? Does the network pattern suggest coordination or coincidence? Is the state-media overlap temporally consistent with a seeding-and-laundering cycle? These are judgement calls that require both financial literacy and doctrinal knowledge, which is why the cell needs people from both worlds.

When a campaign is assessed as probable, the escalation protocol activates. The first step is alerting the relevant financial regulator so that enhanced market surveillance can be applied to

the affected securities. The second is notifying allied partners through the intelligence sharing channel so that parallel monitoring can be activated in other jurisdictions. The third, if the campaign is assessed as large-scale or imminent, is briefing senior policymakers who hold the legal authorities for intervention. The response does not need to be public. In many cases, the most effective countermeasure would be a quiet adjustment to market surveillance parameters that makes the campaign less effective without revealing that it has been detected.

Building this capability also requires a training pipeline that does not currently exist. The analyst who can read a doctrinal signature in a social media cluster while simultaneously interpreting abnormal volume in an options chain is not a person that any single institution currently produces. Intelligence agencies train people to think about adversary intent and campaign structure. Financial regulators train people to think about market microstructure and trading behavior. The analyst this mission requires needs both skill sets, plus enough familiarity with reflexive control doctrine to distinguish a genuine operation from a market that is simply reacting to news. This means joint training programs, second-hand arrangements between intelligence agencies and financial regulators, and a career pathway that rewards cross-domain expertise rather than penalizing people for leaving their home institution. Several allied nations have begun building this kind of hybrid workforce for cyber operations. The same model should be extended to the financial narrative domain before the next crisis forces improvisation.

This is not science fiction. Every element of this capability exists in other domains. Cyber fusion centers operate on exactly this model. Counter-terrorism joint task forces use the same data-ingestion and escalation architecture. What is needed is not new technology or new institutional design. It is the decision to apply proven designs to a new domain. The cost would be modest relative to the budgets already allocated to financial regulation and intelligence collection. The hard part is not building the capability. It is getting the right people in the right room to agree that it is needed.

The Offensive-Defensive Imbalance

Since the early 2000s, allied nations have invested heavily in offensive financial warfare, with the United States leading and partners such as the United Kingdom and Australia building complementary capabilities at varying speeds. They have built sanctions regimes that can isolate entire economies, asset-freezing mechanisms that reach across jurisdictions, and export control architectures that deny access to critical technologies. These tools work. They have become central instruments of Western statecraft in the current era of great-power competition.

The defensive side has received almost no equivalent investment. The cognitive integrity of the very markets that underpin these offensive capabilities is essentially undefended against doctrinal-grade narrative operations. Retail investors who interact with these markets daily have no training, no institutional support, and no warning system. The adversary knows this. Reflexive control was designed for exactly this kind of asymmetry: exploit the gap between what the target thinks it understands and what is actually happening to its decision-making.

The urgency is compounded by the expanding attack surface. The *GameStop* episode in January 2021 demonstrated that coordinated social media activity could move billions of dollars in market capitalization within days.[41] That was organic, retail-driven, and largely legal. It also provides a ready-made retrospective test case: applying the six doctrinal signatures to the GameStop corpus would test whether the framework correctly classifies

organic coordination as non-state activity, providing an important validation baseline. Now imagine the same dynamic harnessed by a state actor with doctrinal training, operational patience, and geopolitical objectives. Commission-free trading platforms have put consequential financial decisions in the hands of tens of millions of people who consume their market information through the same social media channels that state-linked influence operations use for targeting. The democratization of trading, which has been broadly positive for financial inclusion, has also created an attack surface that did not exist a decade ago. Every new retail investor who opens a brokerage account and joins a trading subreddit is a potential target who has no idea the threat exists.

The framework presented here provides a starting point for closing the gap. Six detection patterns derived from sixty years of formalized military doctrine. A convergent evidence design that bridges the intelligence and academic communities. A set of institutional and legal recommendations that map onto existing allied architecture. The doctrine is real. The market effects are measurable. The detection problem is tractable.

The next major geopolitical crisis will have a financial dimension, and that financial dimension will have a narrative component. Whether it is a Taiwan contingency that triggers capital flight from Asian markets, a further escalation of sanctions against Russia, or an energy supply disruption that generates panic selling in European markets, the information environment around the affected securities will be contested ground. State-linked actors will seek to amplify panic, shape trading decisions, and create market conditions that serve their strategic interests. They will do this by using techniques refined over six decades of military doctrine, deployed through channels that billions of people use daily, against targets who have no idea the threat exists. The adversary will not wait for allied nations to build detection capability before operating in that space. They are already there, and they have been there for longer than most policymakers realize.

A limitation of the present analysis should be noted. The doctrinal sources drawn upon here are predominantly English-language translations and secondary accounts of Russian and Chinese military thought. The original Russian-language doctrinal literature, and the classified operational guidance that sits beneath published doctrine, may contain nuances and operational details not captured in the available translations. Future research should prioritize engagement with native-language sources and, where possible, collaboration with scholars who have direct access to the primary doctrinal materials.

The question is not whether to invest in this capability. The question is whether the investment comes before or after the next campaign demonstrates, at scale and in public, that financial markets are as vulnerable to doctrinal-grade psychological operations as any other domain of great-power competition.

Endnotes

[1] Vladimir A. Lefebvre, *Conflicting Structures* (Moscow: Nauka, 1967); S. A. Komov, "On the Methods and Forms of Conducting Information Warfare," *Military Thought*, no. 4 (1997). Lefebvre laid the theoretical foundations for reflexive control as a formal model of adversarial decision-making; Komov later adapted it for information warfare applications.

[2] A. Craig MacKinlay, "Event Studies in Economics and Finance," *Journal of Economic Literature* 35, no. 1 (1997): 13–39; Ekkehart Boehmer, Jim Musumeci, and Annette B. Poulsen, "Event-Study Methodology under Conditions of Event-Induced Variance," *Journal of Financial Economics* 30, no. 2 (1991): 253–272.

[3] BP plc, "BP to Exit Rosneft Shareholding," press release, 27 February 2022. See also Stanley Reed and Clifford Krauss, "BP Will Abandon Its Stake in Rosneft, a Russian Oil Giant," *New York Times*, 27 February 2022.

[4] Price data derived from Bloomberg terminal data covering the event window. The approximately fifteen percent decline in Rosneft's London-listed depositary receipts reflected both the direct impact of divestiture announcements and broader market repricing of Russian sovereign risk.

[5] Executive Order 14066, "Prohibiting Certain Imports and New Investments with Respect to Continued Russian Federation Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine," 8 March 2022. ExxonMobil share price data from Bloomberg.

[6] Werner F.M. De Bondt and Richard Thaler, "Does the Stock Market Overreact?" *Journal of Finance* 40, no. 3 (1985): 793–805. De Bondt and Thaler's foundational study demonstrated that markets systematically overreact to dramatic news, producing predictable reversal patterns that narrative-driven campaigns can exploit.

[7] James J. Tennant, "Detecting Reflexive Control in Financial Markets: An Event Study of Sanctions-Related Information Operations" (working paper, University of Technology Sydney, 2026). Available on request.

[8] The event study methodology and full statistical results are detailed in the companion academic paper and available on request. The study uses standard market model methods following MacKinlay (1997) with cross-sectional significance testing per Boehmer, Musumeci, and Poulsen (1991).

[9] Vladimir A. Lefebvre, *Conflicting Structures* (Moscow: Nauka, 1967).

[10] S. A. Komov, "On the Methods and Forms of Conducting Information Warfare," *Military Thought*, no. 4 (1997).

[11] Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War* (ISW) Russia Report 1 (2015).

[12] For a comprehensive overview, see European External Action Service, "Tackling Disinformation: A Compendium of Activities," updated annually. The U.S. Global Engagement Center, authorized under the National Defense Authorization Act for Fiscal Year 2017, §1287, coordinates counter-disinformation efforts across federal agencies.

[13] Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making," Council of Europe Report DGI (2017)09, 2017. Wardle and Derakhshan distinguish between misinformation (false content shared without harmful intent), disinformation (false content created and shared to cause harm), and mal-information (genuine content shared to cause harm).

[14] Shimon Kogan, Tobias J. Moskowitz, and Marina Niessner, "Social Media and Financial News Manipulation," *Review of Financial Studies* 36, no. 12 (2023): 4809-4849.

[15] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256.

[16] Keir Giles, *Handbook of Russian Information Warfare*, NATO Defense College Fellowship Monograph 9 (2016).

[17] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

[18] Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia* (New York: PublicAffairs, 2014).

[19] Robert J. Shiller, "Narrative Economics," *American Economic Review* 107, no. 4 (2017): 967-1004.

[20] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (2018): 1146-1151.

[21] Brad M. Barber et al., "Attention-Induced Trading and Returns: Evidence from Robinhood Users," *Journal of Finance* 77, no. 6 (2022): 3141–3190.

[22] The Global Database of Events, Language, and Tone (GDELT) is an open-source, real-time dataset that monitors global news media, cataloguing events, sentiment, and source metadata across more than 100 languages. See Kalev Leetaru and Philip A. Schrodt, "GDELT: Global Data on Events, Location, and Tone, 1979–2012," paper presented at the International Studies Association Annual Convention, April 2013.

[23] The concept of "coordinated inauthentic behavior" was formalized by Meta (formerly Facebook) as a

policy framework for identifying state-linked influence operations on its platforms. See Ben Nimmo, "Identifying Coordinated Inauthentic Behavior," Graphika/Atlantic Council Digital Forensic Research Lab, 2020.

[24] Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation," Oxford Internet Institute Working Paper 2019.3 (2019).

[25] Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford: Oxford University Press, 2018).

[26] RT (formerly Russia Today) and TASS are editorially aligned with Russian state policy positions. See European Council Decision 2022/351 of 1 March 2022, which suspended RT broadcasting in the European Union on the grounds that RT is "under the permanent control of the Kremlin."

[27] The Information Office of the State Council, "China's National Defense in the New Era," white paper, July 2019. The "Three Warfares" concept (public opinion warfare, psychological warfare, legal warfare) was formally adopted by the Central Military Commission in 2003.

[28] For English-language analysis of the Three Warfares in practice, see Stefan Halper, *China: The Three Warfares*, report prepared for the Office of Net Assessment, U.S. Department of Defense, May 2013; and Dean Cheng, "Winning Without Fighting: Chinese Legal Warfare," Heritage Foundation Backgrounder no. 2692, 2012.

[29] Ant Group's initial public offering, which would have been the world's largest, was suspended by Chinese regulators in November 2020. See Lingling Wei and Jing Yang, "China's President Xi Jinping Personally Scuttled Jack Ma's Ant IPO," *Wall Street Journal*, 12 November 2020. Didi Global was directed to delist from the New York Stock Exchange in December 2021.

[30] Valery Gerasimov, "The Value of Science Is in the Foresight," *Military-Industrial Courier*, 27 February 2013, translated by Robert Coalson.

[31] SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a Belgian cooperative established in 1973, overseen by the National Bank of Belgium and the G-10 central banks. See Susan V. Scott and Markos Zachariadis, *SWIFT: Cooperative Governance for Network Innovation, Standards, and Community* (London: Routledge, 2014).

[32] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 42-79.

[33] Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: PublicAffairs, 2013).

[34] Office of Personnel Management data breach (2015), *SolarWinds* supply chain compromise (2020), and *Colonial Pipeline* ransomware attack (2021) each accelerated institutional reform in cybersecurity governance.

[35] Executive Order 14028, "Improving the Nation's Cybersecurity," 12 May 2021.

[36] The Cyber Threat Alliance was founded in 2014 as an industry-led platform for sharing threat intelligence across competitors. Its structure offers a model for allied cooperation on financial narrative threats.

[37] Security of Critical Infrastructure Act 2018 (Cth), as amended by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022.

[38] International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §1701-1706. IEEPA grants the President broad authority to regulate economic transactions in response to national security threats.

[39] National Security Act 2023 (UK), c. 32. Part 1 creates new offences for espionage, sabotage, and foreign interference; Part 2 introduces prevention and investigation measures modelled on terrorism prevention orders.

[40] On the tension between national security monitoring and free expression, see Jack M. Balkin, "The Constitution in the National Surveillance State," *Minnesota Law Review* 93, no. 1 (2008): 1–25. For the European framework, see European Convention on Human Rights, Articles 8 (right to privacy) and 10 (freedom of expression). In Australia, the Privacy Act 1988 (Cth) governs the collection and handling of personal information by government agencies.

[41] U.S. Securities and Exchange Commission, "Staff Report on Equity and Options Market Structure Conditions in Early 2021," 14 October 2021. See also Gregory W. Eaton et al., "Zero-Commission Individual Investors, High Frequency Traders, and Stock Market Quality," *Journal of Financial and Quantitative Analysis* (forthcoming).

From Ore to Leverage

Lithium, Threat Finance, and Hybrid Competition

By Bradley A. Mortin

Introduction: Critical Minerals as a Gray-Zone Finance Problem

Strategic competition in the contemporary security environment is increasingly conducted at the sub-threshold level of armed conflict. Rather than relying on overt military force, state and non-state actors (NSAs) increasingly pursue advantage through economic coercion, financial manipulation, and market exploitation with plausible deniability.[1] In this gray-zone context, economic and financial systems have become active instruments of power. Critical-mineral and rare earth element (REE) supply chains, particularly those emerging from fragile and conflict-affected regions, now occupy a central place within this competitive landscape. This article addresses that gap by examining lithium supply chains through a counter-threat finance (CTF) lens, rather than a market or resource-security framework.[2]

Lithium, as a representative critical mineral within the wider REE and strategic-commodities ecosystem, is emblematic of this recent shift. As a foundational input for all battery technology, renewable energy storage, and even advanced defense technologies, lithium is central to national strategies focused on energy transition, industrial resilience, and technological sovereignty.[3] As such, demand continues to accelerate rapidly, yet supply chains remain geographically concentrated, governance-light, and operationally vulnerable.[4] Furthermore, they have also created opportunities for violent NSAs and criminal networks to embed themselves within emerging extraction and transit systems, particularly in regions where state authority is limited and artisanal and small-scale mining (ASM) predominates.[5] Existing CTF and sanctions regimes are optimized to detect and disrupt illicit financial transactions, but not to identify how coercion and violence are monetized through material transformation and global trade. As a result, emerging commodity-based threat-finance systems risk remaining analytically invisible until they have become critically entrenched.[6]

Bradley A. Mortin is a PhD candidate within the Department of War Studies at King's College London, focusing on the geopolitics of collective intelligence in military alliance settings. He holds a BA (Hons) and MA in Intelligence and International Relations from Staffordshire University, an MPhil in Politics and International Studies from Cambridge University, and an MSc in Cyber Defence and Information Assurance from Cranfield University. In addition to this, Bradley maintains a role within the UK Ministry of Defence (MoD) and is both a Chief of the General Staff (CGS) Fellow and Chief of Defence Intelligence (CDI) Fellow.

This article argues that lithium supply chains in the Sahel, the arid belt of land stretching from Northeast to Northwest Africa, should be understood not primarily as development, governance, or regulatory challenges, but as hybrid threat-finance systems operating at the intersection of CTF and threat finance and economic levers (TFEL) of power.[7] In such environments, control over extraction sites, transport corridors, and intermediary actors allows armed groups to convert territorial influence into sustained financial power.[8] Associated revenues generated through coercive taxation, protection arrangements, and smuggling are not incidental by-products of instability; they are central enablers of armed-group resilience, recruitment, and influence activities.[9]

Critically, the risks posed by lithium extend beyond the direct financing of violence. Once lithium-bearing material enters aggregation, processing, and refining stages, it rapidly loses any meaningful traceability to its origin.[10] Through the necessary processes of industrial transformation, lithium becomes financially fungible, enabling value derived from coercion and insecurity to be absorbed into legitimate global markets.[11] From this critical point, supply chains that underpin advanced civilian and military technologies may unknowingly begin to incorporate material linked to armed groups and criminal intermediaries into every aspect of their delivery and operations.[12] The result is a convergence of security and economic risk: violent actors are financed, while states pursuing critical-mineral resilience unwittingly inherit hidden vulnerabilities within their own supply chains.

These dynamics are not unique to lithium, nor are they unprecedented. Comparable mechanisms have long characterized the illicit gold trade in West Africa, where ASM extraction, intermediary networks, and centralized refining have enabled laundering at scale.[13] However, what distinguishes lithium is its strategic timing and significance. Unlike gold, lithium sits at the heart of future energy systems and emerging military capabilities.[14] Allowing lithium supply chains to replicate established threat-finance pathways, therefore, risks embedding instability and coercion within the foundations of future economic and defense power.

Despite growing recognition of critical minerals as strategic assets, policy responses have largely emphasized regulatory compliance, corporate due diligence, and industrial policy.[15] While necessary, these approaches are insufficient on their own. From a CTF and TFEL perspective, lithium supply chains, as representatives of wider critical-mineral and REE systems, are not merely vulnerable but actively exploitable as instruments of hybrid warfare and strategic competition.

To develop these claims, the article first places lithium within a conceptual framework that links CTF, TFEL, and hybrid warfare. It then proceeds by analyzing the mechanisms through which critical-mineral supply chains become threat-finance systems, drawing comparative evidence from existing gold-smuggling networks to demonstrate a proof-of-pattern. The article concludes by identifying priority financial-intelligence indicators and proposing actionable CTF measures, each designed to deny adversaries revenue and leverage while also safeguarding these supply chains in this new era of persistent strategic competition.

Conceptual Framework: Counter Threat Finance, Economic Leverage, and Hybrid Warfare

Understanding how lithium supply chains can function as instruments of strategic competition requires a level of conceptual clarity regarding the relationship between economic warfare, financial warfare, CTF, and TFEL. Though often treated separately, sub-threshold conflict now shows increasing convergence. This section develops a framework that situates critical-mineral supply

chains within existing concepts of hybrid warfare, explaining why lithium should be treated not only as a strategic resource but also as a financial and economic weapon.

Economic Warfare and Financial Warfare in Contemporary Competition

Economic warfare traditionally refers to the use of economic instruments (trade controls, embargoes, market access restrictions, and resource denial) as the means of coercing adversaries or shaping their strategic choices.[16]

Critical minerals such as lithium exemplify this identified convergence. Control over extraction, processing, or transit affects not only material availability but also factors related to price stability, investment confidence, and long-term dependence.[17] When violent NSAs and criminal networks embed themselves within these systems, economic and financial warfare ceases to be a tool exclusively for state use, instead becoming accessible to a range of actors operating outside formal political authority.[18]

Counter Threat Finance and Threat Finance and Economic Levers of Power

U.S. CTF doctrine, as articulated in Department of War guidance, has historically focused on identifying and disrupting the financial networks that sustain terrorist organizations and insurgents, emphasizing the denial, disruption, and degradation of adversary value generation rather than broader economic leverage.[19] The primary tools at its disposal (financial tracking, asset freezes, sanctions, and cooperation with regulated financial institutions) have been particularly effective against instances of threat finance that rely on cash movement or formal banking channels.[20] However, these approaches are much less effective when value is generated and transferred through commodities rather than money. This distinction matters as it directs analytical attention beyond illicit financial transactions toward the material and commercial processes through which coercion and violence are converted into sustainable economic power.

By contrast, UK doctrine conceptualizes TFEL as the use and manipulation of economic and financial systems themselves as instruments of national power, extending beyond the disruption of adversary finance to the creation of strategic advantage and imposed cost.[21] Rather than concentrating solely on how adversaries raise funds, TFEL emphasizes how control, influence, or manipulation of economic and financial systems can be used deliberately to impose cost, shape behavior, and generate strategic advantage.[22] Under its direction, revenue generation, coercive leverage, and systemic vulnerability no longer exist as separate outcomes, but rather as interlinked features of the same underlying structures.

This dynamic is also visible in lithium supply chains. At the local level, armed groups extract revenue through coercive taxation, access control, or protection arrangements at sites of ASM.[23] At the regional level, intermediaries and smuggling networks facilitate the movement of the mined lithium across borders and into aggregation points.[24] Finally, at the global level, the act of processing and refinement converts the raw lithium into standardized outputs, erasing provenance and enabling integration into legitimate markets.[25] Each stage simultaneously generates income for armed actors (at different levels) and embeds risk within the international economic system. This is not merely terrorist financing in the narrow sense, but a much broader concept that incorporates the exploitation of economic networks as levers of power in strategic competition, a shift increasingly emphasized in contemporary CTF scholarship.[26]

Therefore, reframing lithium as a TFEL asset shifts the central analytic question so that the concern is no longer simply how much revenue armed

groups derive from critical minerals, but also how their participation in these supply chains shapes strategic dependencies, resilience, and vulnerability within broader competitive dynamics.

Hybrid Warfare and Plausible Deniability Below the Threshold

Hybrid warfare is characterized by the coordinated use of military, economic, informational, and criminal tools that jointly work to achieve strategic objectives whilst also seeking to avoid the risk of escalation into open conflict.[27] A defining feature of hybrid approaches is plausible deniability, achieved through the use of proxies, intermediaries, and ostensibly civilian or commercial activity, enabling state and proxy actors to pursue strategic objectives without direct attribution.[28] Financial and economic systems are particularly well-suited to this mode of competition as they allow influence to be exercised without attribution, and effects to be generated without visible violence.[29]

Commodity supply chains function naturally as hybrid-warfare enablers, reflecting the broader convergence of licit and illicit economic activity, criminal networks, and security threats observed across contemporary conflict environments.[30] They combine licit and illicit actors, can operate across jurisdictions with uneven regulatory capacity, and rely on commercial norms that prioritize efficiency over scrutiny.[31] In fragile environments, these characteristics also allow armed groups to function as economic participants rather than overt belligerents, embedding themselves within markets rather than confronting states directly.[32]

Across the Sahel, lithium extraction and transit occur within precisely such conditions. Weak governance, porous borders, and reliance on ASM create environments in which coercion and commerce coexist.[33] In such situations, armed groups can extract revenue while simultaneously remaining formally outside the global financial system, relying on commodity transformation and trade-based laundering to realize value.[34] This allows these actors to sustain operations, fund influence activities, and adapt to external pressures, all without triggering the visibility associated with conventional financial flows.

From a strategic perspective, this reality blurs the line between crime, insurgency, and competition. It also complicates responses at the regional and international level. Tools designed for counterinsurgency, sanctions enforcement, or development assistance are each insufficient, as the threat resides outside any single domain. Therefore, instead, lithium supply chains must be understood as hybrid systems through which economic, financial, and security dynamics have come to reinforce one another.

Analytical Implications

The framework formed thus far yields three key implications that guide the remainder of the article. Firstly, effective CTF responses must extend beyond financial institutions alone, to address commodity transformation, trade-based laundering, and intermediary networks. Secondly, assessments of critical-mineral security must also incorporate threat-finance risk alongside more traditional concerns regarding supply disruption and market concentration. And thirdly, hybrid-warfare analysis must also account for how economic systems can generate both revenue and strategic leverage simultaneously.

Taken together, these three insights support a reframing of lithium as a financially mediated economic lever rather than a neutral, industrial input. The following section applies this framework directly to the mechanics of lithium supply chains in fragile environments, demonstrating how localized coercion, material transformation, and market integration interact to produce threat-finance systems that generate both revenue and strategic leverage below the threshold of armed conflict.

From Ore to Leverage: How Lithium Supply Chains Become Threat-Finance Systems

Lithium supply chains formed in fragile environments do not become sources of threat finance through isolated criminal acts. Rather, they evolve into threat-finance systems when structural conditions, such as weak governance, high commodity value, fragmented oversight, and centralized processing, combine to allow violent NSAs and criminal intermediaries to convert territorial influence into financial power and strategic leverage. The central mechanism is not illicit finance at any single point, but the cumulative transformation of coercion into legitimate economic value as lithium moves through successive stages of the supply chain.[35]

In most states and regions of the Sahel, lithium extraction occurs through ASM, characterized by informality, limited state presence, and a reliance on local power brokers.[36] These conditions are extremely conducive to armed-group exploitation. It minimizes operational exposure, avoids the need for technical expertise or capital investment, and embeds armed actors within local economies rather than positioning them as overt adversaries of the state. Crucially, it also produces revenue streams that are both reliable and long-lasting.[37] From a threat-finance perspective, persistence matters more than scale.[38] At this stage, value is generated through territorial control and coercion rather than financial exchange, leaving a minimal transactional footprint for conventional financial intelligence systems to detect or disrupt.

Implication: For CTF practitioners, this underscores why lithium-based threat finance is resilient. Disruption strategies that focus solely on high-value transactions or downstream financial flows will likely miss the steady, low-visibility revenue that is extracted at the point of production.

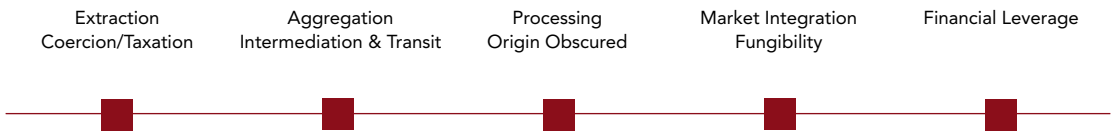
Aggregation and Transit: Intermediaries as Buffers and Enablers

Once extracted, lithium-bearing material enters aggregation and transit networks that further distance the armed groups from downstream markets. At this stage, documentation is likely to be incomplete, inconsistent, or deliberately misleading, particularly in regions with weak customs enforcement or endemic corruption.[39]

Smuggling in this context is not always clandestine. It frequently exploits regulatory asymmetries rather than simply evading borders entirely.[40] Under these circumstances, each transactional handoff reduces traceability and increases deniability.

Material collected from multiple ASM sites is purchased by local traders operating on thin margins, often using cash, in-kind exchanges, or informal credit arrangements that leave little documentary trace.[41] As material is pooled and resold through successive intermediaries, provenance is progressively diluted despite the absence of overtly illicit transactions. By the time lithium reaches an

Figure 1. Extraction: Coercion, Informality, and Revenue Stability



Source: Author

aggregation hub or transit state, its value has already been realized locally, while responsibility for origin verification has been diffused across multiple actors. Financial transactions, where they occur, reflect routine commercial activity rather than the underlying coercion that enabled production. In this way, intermediaries transform localized violence into market-ready outputs, without requiring overt laundering or centralized coordination.

Intermediaries also play a dual role. They shield armed groups from scrutiny while enabling access to broader markets. At the same time, they introduce systemic opacity that complicates almost all forms of financial intelligence collection. Because value is consolidated through physical aggregation and informal brokerage rather than discrete financial transactions, attribution becomes diffused, and financial monitoring tools lose analytical resolution at this stage.[42]

Implication: Effective CTF responses must prioritize mapping and disrupting intermediary networks. Focusing on producers or end-users alone leaves the most adaptive and least visible elements of the system, the actors, untouched.

Processing and Refining: Industrial Transformation as Laundering

The processing and refining stage represents the most consequential transformation in lithium-based threat finance. At this point, lithium transitions from a locally sourced material output into a standardized, market-ready input. Physical processing eliminates origin markers, while associated financial transactions appear indistinguishable from legitimate trade.[43]

These facilities are economically indispensable yet frequently operate with limited upstream scrutiny. Once illicitly sourced lithium enters this stage, it becomes functionally indistinguishable from licit production. This laundering effect is structural, embedded in industrial norms that prioritize throughput over security risk.[44]

From a CTF perspective, processing facilities perform a role analogous to financial intermediaries in traditional money-laundering networks. They convert high-risk inputs into low-risk outputs, enabling integration into formal markets without triggering any conventional controls. Processing, therefore, functions as a structural laundering mechanism, severing traceability to coercive origins and rendering downstream financial flows indistinguishable from legitimate commercial activity, significantly hampering any forms of financial intelligence collection.

Implication: Processing and refining nodes represent high-leverage intervention points. CTF efforts that fail to engage at these stages risk allowing illicit value to be normalized before any financial red flags can be applied.

Market Reintegration and Financial Fungibility

After processing, lithium enters global markets as a fungible commodity. It is traded, financed, and incorporated into supply chains alongside licit material. At this stage, differentiation based on origin is functionally impossible and no longer required, benefiting armed groups indirectly through earlier payments, revenue-sharing arrangements, or equity interests mediated by intermediaries.[45]

This point of integration represents the completion of the threat-finance cycle. Territorial control exercised at the point of extraction has been translated, through commercially routine transactions, into financial power that can then be deployed across multiple domains. The system's resilience lies in its normalcy, where each transaction appears rational, legal, and detached from violence, even as the aggregate effect sustains armed actors and embeds instability within strategic supply chains. Once value circulates through licit trade and investment channels at this stage, it falls largely outside the scope of counter-threat finance tools that are

designed to identify illicit finance rather than structurally embedded economic risk.[46]

From Revenue to Leverage: Strategic Consequences

The significance of lithium-based threat finance extends beyond simply funding armed groups. By embedding illicitly sourced material into global supply chains, these networks create strategic dependencies and reputational risks for all downstream consumers. States pursuing critical-mineral diversification may inadvertently incorporate material linked to coercion and violence into their systems, undermining supply-chain resilience and introducing latent strategic vulnerability.

Because lithium underpins future energy systems and emerging military technologies, these dynamics acquire strategic weight. Threat-finance networks operating through lithium supply chains do not merely sustain violence; they shape the competitive environment in which states are required to operate. Revenue generation and leverage creation are inseparable, and this dual effect distinguishes lithium as a TFEL asset rather than a conventional funding stream.

Understanding this mechanism explains why traditional CTF tools struggle against commodity-based threat finance and why intervention must therefore target transformation points, intermediaries, and trade-based laundering, rather than financial endpoints alone. The next section demonstrates that these dynamics are not unique to lithium by examining comparable mechanisms in the established illicit gold trade, providing empirical proof-of-pattern for the argument advanced here.

Comparative Evidence: Gold Smuggling as Proof-of-Pattern in Commodity-Based Threat Finance

Gold is examined here not as a predictive analogue for lithium, but as a mature example of how commodity supply chains with similar structural characteristics can evolve into durable threat-finance systems over time. The threat-finance dynamics emerging around lithium in the Sahel are not novel. Instead, they reflect mechanisms that have long characterized the illicit gold trade across West Africa, where extraction through ASM, intermediary networks, and centralized refining have all enabled sustained revenue generation for armed groups and criminal actors. As such, gold provides a mature empirical case demonstrating how informal extraction, intermediary aggregation, and centralized processing evolve into resilient threat-finance systems.

Gold is particularly pertinent in this argument as a comparator due to sharing several structural characteristics with lithium. Both commodities exhibit high value-to-weight ratios, widespread extraction through ASM, particularly in Africa, and limited traceability once processed. Both also move through transnational supply chains that span jurisdictions with varying regulatory capacities. Crucially, gold's longer history of exploitation also allows observation of how such systems mature over time, indicating lithium's likely trajectory without targeted intervention.

Artisanal Extraction and Armed-Group Revenue

As with lithium, violent NSAs and groups rarely manage extraction directly. Instead, they extract value through coercive taxation, protection arrangements, and control over access to mining sites.[47] These practices generate predictable income streams while minimizing operational exposure.

From a CTF perspective, the gold trade demonstrates that modest but persistent revenues can sustain armed groups over enduring periods of time. The strategic importance of such income lies not in scale, but in durability. This pattern closely mirrors the dynamics observed in emerging regions of

lithium extraction, reinforcing the assessment that lithium-based threat finance is likely to be resilient once established.

Intermediaries, Transit States, and Jurisdictional Arbitrage

Illicit gold rarely moves directly from mine to market. Instead, it passes through layers of intermediaries, from local traders, transporters, and brokers, each of whom aggregates production from multiple sites and blends licit and illicit material.[48] Gold is then moved into transit states that function as gateways into global markets, exploiting differences in export controls, taxation, and customs enforcement in a manner that proves beneficial to nefarious actors.[49]

This jurisdictional arbitrage is central to laundering. Each handoff erodes traceability and disperses responsibility, making downstream attribution increasingly difficult. The resulting opacity is not accidental; it is a structural feature of commodity-based threat finance. Here, lithium supply chains exhibit the same reliance on intermediaries and regulatory fragmentation as gold, suggesting that similar arbitrage opportunities will persist unless deliberately addressed.

Refining Hubs as Laundering Chokepoints

The refining stage is the most decisive transformation in the illicit gold trade. Once gold enters major refining hubs, it is melted and recast into standardized forms, eliminating any remaining indicators of its provenance.[50]

Refining hubs thus function as laundering chokepoints analogous to correspondent banks in traditional money-laundering networks. They convert high-risk input into low-risk output, enabling integration into formal markets. As with lithium, the critical mechanism is not extraction itself but the conversion of coercively produced material into standardized, fungible inputs through aggregation and processing, at which point threat-derived value becomes indistinguishable from licit supply. Yet, despite this reality, these nodes have historically faced only limited scrutiny regarding upstream sourcing, particularly when operating in jurisdictions that prioritize commercial throughput.[51]

This pattern is also directly applicable to lithium. Processing and refining facilities for critical minerals perform the exact same structural function, transforming raw material into fungible industrial inputs while obscuring origin. Gold thus demonstrates that once laundering at this stage becomes entrenched, any disruption becomes exponentially more difficult to achieve.

Implications for Lithium and Critical-Mineral Security

The gold trade provides clear proof-of-pattern for the risks posed by lithium supply chains in fragile regions. The same structural conditions, informal extraction, intermediary-driven aggregation, jurisdictional arbitrage, and centralized processing are all present in emerging lithium markets. Gold-based threat-finance systems are mature and deeply embedded, whilst lithium systems remain in their infancy. This distinction matters because maturity determines both the resilience of threat-finance systems and the feasibility of disruption, making lithium supply chains a rare case where preventive intervention remains possible before patterns of normalization harden.

This temporal distinction is strategically significant. It suggests that early, targeted CTF interventions focused on processing nodes, intermediary networks, and trade-based laundering indicators still have time to prevent lithium supply chains from replicating the resilience now observed in the gold trade. Conversely, any failure to act risks allowing lithium to follow the same trajectory as gold, embedding threat finance within lithium supply chains, central to future energy and defense systems.

Figure 2. Gold and Lithium: Commodity Threat-Finance Comparison

Feature	Gold	Lithium
ASM prevelance	High	Emerging
Role of intermediaries	Extensive	Growing
Processing concentration	High	High
Traceability after processing	Low	Low
Threat-finance maturity	Entrenched	Formative

Source: Author

By demonstrating that commodity-based threat finance operates through repeatable mechanisms, the gold case strengthens the argument for lithium in that it should be treated as a TFEL asset. It also underscores the urgency of adapting CTF tools to address commodities not simply as peripheral enablers of violence, but as core components of hybrid warfare and strategic competition. The gold comparison demonstrates that commodity-based threat finance follows repeatable pathways that routinely evade transaction-focused financial intelligence, reinforcing the need to adapt CTF analysis towards supply-chain dynamics and trade-based mechanisms.

Financial Intelligence Implications: Detecting Commodity-Based Threat Finance

Lithium-based threat finance presents a fundamentally different detection problem from other forms of traditional terrorist financing. As a result, any effective detection depends less on tracing individual transactions and more on identifying systemic anomalies across trade, logistics, and industrial processes. This section outlines the implications of lithium-based threat finance for financial intelligence (FININT) collection, analysis, and operational prioritization.

Why Traditional CTF Models Are Insufficient

Traditional CTF frameworks assume that value transfer ultimately manifests as a financial transaction that can be detected, disrupted, or sanctioned. In lithium supply chains, this assumption is harder to maintain. By the time revenue begins to enter the formal economy, it is already recorded as legitimate commercial income, divorced from the conditions under which the commodity was produced.[52]

Moreover, the industrial transformation of lithium undermines traceability. Processing and refining eliminate physical indicators of origin, while associated financial records reflect lawful trade between commercial entities.[53] This disconnect renders conventional "follow-the-money" approaches inadequate on their own. Instead, lithium-based threat finance requires a "follow-the-system" analytical approach that treats the supply chain itself as the primary object of intelligence. This represents a fundamental shift in FININT logic, from retrospective detection of illicit finance to prospective identification of structural risk, embedded in each element of production, trade, and processing.

Implication: FININT units that rely exclusively on banking data will systematically under-detect commodity-based threat finance, even as armed actors generate sustained revenue.

Priority Indicators for FININT and CTF Analysts

Despite these critical challenges, lithium-based threat finance produces detectable patterns when analyzed at the system level. Priority indicators include:

- **Trade Discrepancies:** Persistent mismatches between reported exports from extraction regions and the imports recorded by transit or processing states.
- **Processing Concentration Risk:** Heavy reliance on limited processing or refining facilities that accept material from high-risk regions with only minimal upstream due diligence.
- **Anomalous Transport Routes:** Use of indirect, inefficient, or non-intuitive routing that bypasses established export corridors, suggesting the deliberate avoidance of scrutiny.
- **Intermediary Volatility:** Frequent changes in traders, brokers, or transport firms, or a reliance on newly incorporated entities with only limited operational history.
- **Documentation Irregularities:** Recurrent inconsistencies in mining licenses, export permits, or certificates of origin issued by authorities with limited verification capacity.
- **Pricing and Payment Anomalies:** Sales at below-market prices, in-kind payments, or complex offset arrangements that obscure the true value of a transfer.

Taken together, these indicators are most effective when applied as part of a pattern-recognition framework, where risks emerge from correlations across datasets rather than from single-source confirmation. Each of these indicators highlights the need for widespread integration of customs data and systems, trade statistics, corporate registries, and open-source reporting, all into shared FININT workflows.

Collection and Analytic Challenges

Commodity-based threat finance exposes structural limitations within existing intelligence architectures. These limitations, rather than being analytical capacity alone, represent the primary obstacle to detecting commodity-based threat finance at scale. Corporate secrecy, opaque ownership structures, and the use of front companies also further complicate forms of attribution.[54]

Analytically, lithium-based threat finance benefits significantly from normalization. Because illicit material will always need to be blended with licit production and processed through legitimate facilities, yet traditional threshold-based alerts are ineffective. Analysts must instead adopt a network-centric approach, mapping out relationships among extraction sites, intermediaries, processing hubs, and financial endpoints. This deeper look into the first stages of the supply chain requires sustained analytic investment and institutional support that many CTF structures are not currently designed to provide.

Implication: Without organizational adaptation, FININT units risk treating lithium-based threat finance as a peripheral issue rather than a systemic vulnerability.

Adapting FININT to Hybrid Economic Threats

Detecting lithium-based threat finance requires expanding the scope of FININT beyond money flows to include both economic and industrial intelligence.

From a strategic-competition perspective, FININT should be tasked not only with identifying illicit revenue streams but also with assessing how commodity flows generate leverage, dependency, and vulnerability. In this sense, FININT becomes the early-warning function for economic coercion and hybrid influence, rather than a narrowly reactive tool focused on financial crime. Lithium supply chains are not merely sources of funding; they are components

of hybrid systems that shape the strategic environment. Intelligence that fails to capture this dual function risks being strategically incomplete.

The following section translates these analytical insights into concrete CTF options. These options focus on adapting existing CTF authorities and partnerships to intervene earlier in commodity supply chains, where threat-finance systems remain most vulnerable, while simultaneously safeguarding critical-mineral supply chains.

Counter Threat Finance Options for Lithium-Based Supply Chains

If lithium supply chains are understood as threat-finance systems and economic levers of power, CTF responses must be recalibrated accordingly. Effective disruption, therefore, requires targeting the key points of normalization, intermediation, and leverage that allow illicitly sourced lithium to be absorbed into global markets. This section outlines prioritized CTF lines of effort, highlighting both their strategic value and associated trade-offs. The ordering of these lines of effort reflects their relative leverage over threat-finance systems, rather than their ease of implementation or political convenience.

Priority Line of Effort: Processing and Refining Nodes

Processing and refining facilities represent the highest-leverage intervention point within lithium-based threat-finance systems. Once illicit lithium passes through this stage, downstream disruption becomes significantly more difficult. Intervening at this point, therefore, offers disproportionate returns, as it disrupts both revenue realization and the normalization process that shields illicit value from detection.

CTF-relevant measures should thus prioritize enhanced due-diligence requirements for processors sourcing from high-risk regions, including origin verification, supplier audits, and risk-based inspections. Where voluntary compliance proves insufficient, states should employ regulatory penalties or financial restrictions tied to sourcing practices.

Trade-off: Stricter oversight may increase costs and slow throughput, potentially affecting short-term supply objectives. However, failure to act risks embedding practices of coercion and instability within supply chains that are central to future energy and defense systems.

Secondary Line of Effort: Trade-Based Money Laundering Controls

Strengthening trade-based money laundering (TBML) controls requires closer integration between CTF practitioners and customs authorities.[55] In this context, FININT functions less as a trigger for enforcement and more as an enabling capability that prioritizes where scarce customs and inspection resources are applied.

Here, multijurisdictional data-sharing is also particularly important. Many anomalies only become visible when data from both export and import sources is compared across borders. Coordinated targeting also reduces displacement effects, whereby illicit flows shift routes in response to the numerous forms of unilateral enforcement.

Trade-off: Enhanced TBML controls require sustained interagency cooperation and data integration, which may strain institutional capacity. Nonetheless, these measures directly address the mechanisms that allow threat finance to continue to persist undetected.

Disrupting Intermediary Networks and Facilitators

Intermediaries are central to lithium-based threat finance. Brokers, transport firms, and front companies all insulate armed groups from

scrutiny while enabling the blending of licit and illicit material. CTF efforts should therefore prioritize mapping and disrupting intermediary networks rather than focusing exclusively on producers or end-users. Because intermediaries often service multiple supply chains simultaneously, disruption at this level can generate cascading effects across commodities, regions, and threat-finance networks. Targeted designations, licensing restrictions, or asset freezes against repeat facilitators can also have cascading effects across supply chains.

Trade-off: Action against intermediaries may face legal and evidentiary hurdles, particularly where activities fall into regulatory gray zones. However, intermediaries represent some of the most adaptive and influential nodes within threat-finance systems.

Allied and Partner Coordination

Because lithium supply chains are inherently transnational, unilateral CTF measures are unlikely to succeed in isolation. Effective responses depend on coordination among allies and partners to harmonize due-diligence standards, share intelligence, and align enforcement priorities. Absent coordination and unilateral CTF measures risk displacing illicit flows rather than reducing them, undermining both effectiveness and political sustainability. Capacity-building initiatives aimed at partner states (particularly those along transit routes) can further reduce systemic vulnerabilities and embed CTF considerations.

Trade-off: Multilateral coordination is time-consuming and politically complex, but it is essential to prevent displacement and ensure a long-lasting, durable impact.

Integrating CTF into Strategic Competition and Economic Security

Finally, lithium-based threat finance should be addressed as a strategic-competition problem rather than a narrow issue of counterterrorism. In this framing, CTF becomes a tool for shaping the competitive environment and denying adversaries both revenue and the ability to weaponize economic dependencies below the threshold for armed conflict. Denying armed groups' access to commodity-derived revenue simultaneously reduces their operational capacity whilst also limiting the ability of adversarial actors to exploit supply-chain vulnerabilities for leverage.

CTF practitioners, economic-security policymakers, and industrial regulators must all be coordinated with one another to ensure that threat-finance considerations inform decision-making about sourcing, investment, and diversification. While such integration may introduce short-term friction, it strengthens long-term resilience and denies adversaries the unchallenged opportunity to exploit critical-mineral dependencies.

Together, these lines of effort demonstrate that countering lithium-based threat finance is both feasible and strategically valuable. By shifting focus from financial endpoints to the economic systems that generate and normalize illicit value, CTF can remain an effective instrument for countering hybrid threats and safeguarding strategic supply chains in an era of persistent competition.

Conclusion: Countering Threat Finance at the Level of the Supply Chain

Strategic competition in the contemporary security environment is increasingly waged through economic systems rather than overt military confrontation. As this article has demonstrated, lithium supply chains emerging from fragile regions such as the Sahel function as integrated threat-finance

systems, converting localized coercion into sustained revenue and strategic leverage below the threshold of armed conflict. Through ASM extraction, intermediary networks, and centralized processing, localized coercion is converted into globally fungible value, enabling violent NSAs to sustain operations whilst also embedding instability within the supply chains that underpin future energy and defense capabilities.

Reframing lithium as a form of finance, rather than merely a resource, clarifies why existing policy responses remain insufficient. Regulatory compliance, corporate due diligence, and industrial diversification are all necessary components of critical-mineral strategy but individually fail to fully address the core threat-finance mechanisms that allow illicit value to be normalized through industrial transformation and trade. Traditional CTF approaches that focus tightly on financial transactions are similarly ill-suited to disrupt value transfer embedded in physical commodities and supply-chain infrastructure. The central failure lies not in implementation, but in analytic framing: treating commodities as peripheral enablers rather than as primary vehicles of threat finance obscures where leverage is generated.

The implications of this problem extend far beyond counterterrorism. Lithium-based threat finance illustrates how economic systems can also be exploited as instruments of hybrid warfare, generating revenue, leverage, and plausible deniability, all simultaneously. In this context, CTF is not merely a supporting activity but a form of necessary strategic statecraft. When applied at the level of supply chains rather than transactions, CTF becomes a means of shaping competitive environments, not just reacting to illicit behavior. Denying armed groups and their enablers access to commodity-derived value reduces their operational capacity while also safeguarding economic resilience and limiting adversarial leverage in strategic competition.

The comparative evidence provided from the gold trade underscores the urgency of early intervention. Once commodity-based threat-finance systems mature and normalize, disruption becomes increasingly costly and politically complex. However, lithium supply chains remain in a formative phase, presenting a narrowing but meaningful window for preventive action. The experience of gold demonstrates that once normalization is complete, options contract rapidly, and intervention shifts from prevention to containment. Targeted engagement at processing nodes, coordinated trade-based controls, and systematic disruption of intermediary networks can all help prevent critical minerals from following the same entrenched trajectory observed in illicit gold markets.

As demand for lithium accelerates, failure to adapt CTF to the realities of commodity-based hybrid warfare risks allowing future energy and defense systems to be partially underwritten by coercion and instability. Conversely, integrating CTF into critical-mineral and economic-security strategies offers an opportunity to deny adversaries both revenue and leverage while also strengthening resilience below the threshold of armed conflict. In an era where strategic competition increasingly turns on control of value rather than territory, effective counter-threat finance will depend not on following money alone, but on understanding and disrupting the supply chains through which it is created.

Endnotes

[1] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 42–79, https://doi.org/10.1162/isec_a_00351.
[2] United Nations Security Council Counter-Terrorism Committee Executive Directorate, Concerns over the Use of Proceeds from the Exploitation, Trade, and Trafficking of Natural Resources for the Purposes of Terrorism Financing, CTED Trends Alert (New York: United Nations, 2022), https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jun/cted_cft_trends_alert_june_2022.pdf; U.S. Department of Defense. *Commander's Handbook for Counter Threat Finance* (Washington, DC: Department of Defense, 2011). https://info.publicintelligence.net/DoD-CounterThreatFinance.pdf.
[3] International Energy Agency (IEA), *The Role of Critical Minerals in Clean Energy Transitions*, World Energy Outlook Special Report (Paris: International Energy Agency, 2022), 287, https://iea.blob.core.windows.net/assets/ffd2a83b-8c30-4e9d-980a-52b6d9a86fdc/TheRoleofCriticalMineralsinCleanEnergyTransitions.pdf.
[4] Juan Tan and Jakob Kløve Keiding, *The Cobalt and Lithium Global Supply Chains: Status, Risks and Recommendations*, MiMa Rapport 2023/3 (Center for Minerals and Materials (MiMa) under The Geological Survey of Denmark and Greenland (GEUS), 2023), 146, https://data.geus.dk/pure-pdf/MiMa-R_2023_03_web.pdf.
[5] Gavin Hilson et al., "Artisanal and Small-Scale Mining (ASM) in Sub-Saharan Africa: Re-Conceptualizing Formalization and 'Illegal' Activity," *Geoforum* 83 (2017): 80–90, https://doi.org/10.1016/j.geoforum.2017.05.004.
[6] United Nations Office on Drugs and Crime (UNODC), *Minerals Crime: Crimes in the Supply Chains of Critical Energy Transition Minerals* (Vienna: United Nations, 2025), 63, https://www.unodc.org/documents/data-and-analysis/Crimes%20on%20Environment/Minerals_Crime/Critical_minerals_2025.pdf.
[7] UK Ministry of Defence, *Joint Doctrine Note 2/20: Threat Finance and the Economic Levers of Power* (London: Ministry of Defence, 2020), https://assets.publishing.service.gov.uk/media/5fb7d81fd3bf7f5734b9b5fa/20201119-JDN_2_20_TFEL_web_secure.pdf.
[8] Achim Wennmann, "Economic Dimensions of Armed Groups: Profiling the Financing, Costs, and Agendas and Their Implications for Mediated Engagements," *International Review of the Red Cross* 93, no. 882 (2011): 333–52, https://doi.org/10.1017/S1816383111000361.operational costs, and economic agendas of armed groups and brings together examples from Angola, Kosovo, Sudan, Colombia, and other places. It emphasizes that information about available financing and operational costs is critical for assessing the financial and operational strength of an armed group. It also highlights the need to understand armed groups in the broader context of their evolution and the changes that organizational and territorial expansions require with regards to financing strategies. Overall, the economic dimensions of armed groups should be approached with an open mind so that issues such as financing, costs, and economic agendas can be perceived as opportunities, and not necessarily as a problem for peace.","container-title":"International Review of the Red Cross","DOI":"10.1017/S1816383111000361","ISSN":"1816-3831, 1607-5889","issue":"882","journalAbbreviation":"Int. rev. Red Cross","language":"en","license":"https://www.cambridge.org/core/terms","page":"333-352","source":"DOI.org (Crossref
[9] Louise I. Shelley, *Dirty Entanglements: Corruption, Crime, and Terrorism* (Cambridge: Cambridge University Press, 2014), https://doi.org/10.1017/CBO9781139059039.corruption, and terrorism now deserves high-level policy attention because of its growth trajectory. Using lively case studies, this book analyzes the transformation of crime and terrorism and the business logic of terrorism. Louise I. Shelley concludes that corruption, crime, and terrorism will remain important security challenges in the twenty-first century as a result of economic and demographic inequalities in the world, the rise of ethnic and sectarian violence, climate change, the growth of technology, and the failure of nineteenth- and twentieth-century institutions to respond to these challenges when they emerged.","edition":"1","ISBN":"978-1-107-01564-7","license":"https://www.cambridge.org/core/terms","note":"DOI: 10.1017/CBO9781139059039","publisher":"Cambridge University Press","source":"DOI.org (Crossref
[10] IEA, *The Role of Traceability in Critical Mineral Supply Chains*, IEA/OECD 2025. CC BY 4.0. (International Energy Agency (IEA), 2025), 78, https://iea.blob.core.windows.net/assets/aa827202-9d85-4805-b3ac-d489d3b900e3/TheRoleofTraceabilityinCriticalMineralSupplyChains.pdf; Svenja Schöneich et al., "Traceability and Foreign Corporate Accountability in Mineral Supply Chains," *Regulation & Governance* 17, no. 4 (2023): 954–69, https://doi.org/10.1111/rego.12527.

[11] UNCTAD, *Critical Minerals Boom: Global Energy Shift Brings Opportunities and Risks for Developing Countries* (United Nations Conference on Trade and Development (UNCTAD), 2024), Online, https://unctad.org/news/critical-minerals-boom-global-energy-shift-brings-opportunities-and-risks-developing-countries.
[12] UNODC, *Minerals Crime.*
[13] Marcena Hunter, *Beyond Blood: Gold, Conflict and Criminality in West Africa* (Geneva: Global Initiative Against Transnational Organized Crime, 2022), 61, https://globalinitiative.net/wp-content/uploads/2022/11/Marcena-Hunter-Beyond-blood-Gold-conflict-and-criminality-in-West-Africa-GI-TOC-November-2022.pdf; UNODC, *Gold Trafficking in the Sahel*, Transnational Organized Crime Threat Assessment (TOCTA) (United Nations Office on Drugs and Crime (UNODC), 2024), https://www.unodc.org/documents/data-and-analysis/tocta_sahel/TOCTA_Sahel_Gold_v5.pdf.
[14] Joseph Webster, "Batteries as a Military Enabler," *War on the Rocks*, April 2024, https://warontherocks.com/.
[15] European Union, *Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859*, *Official Journal of the European Union* (2024), https://eur-lex.europa.eu/eli/dir/2024/1760/oj/eng; HM Government, Resilience for the Future: The United Kingdom's Critical Minerals Strategy (London: Her Majesty's Stationery Office, 2024), https://assets.publishing.service.gov.uk/media/62f36bafe90e07714288b188/resilience_for_the_future_the_uks_critical_minerals_strategy.pdf.
[16] Edward N Luttwak, "From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce," *The National Interest* 20 (1990): 17–23.
[17] IEA, *The Role of Critical Minerals in Clean Energy Transitions.*
[18] CTED, *Concerns over the Use of Proceeds from the Exploitation, Trade, and Trafficking of Natural Resources.*
[19] U.S. Department of Defense. *Commander's Handbook for Counter Threat Finance.*
[U.S.] Department of Defense. *DoD Directive 5205.14: DoD Counter Threat Finance (CTF) Policy* (Washington, DC: Department of Defense, 2017), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520514p.pdf.
[20] U.S. Department of the Treasury, *2024 National Terrorist Financing Risk Assessment* (Washington, DC: Department of the Treasury, 2024).
[21] Robert D. Blackwill and Jennifer M. Harris, *War by Other Means: Geoeconomics and Statecraft* (Cambridge, MA: Harvard University Press, 2016); Christopher Clayton et al., *Putting Economics Back into Geoeconomics*, NBER Working Paper no. 33681 (Cambridge, MA: National Bureau of Economic Research, 2025), https://doi.org/10.3386/w33681; UK Ministry of Defence, *JDN 2/20*, 15.
[22] Farrell and Newman, "Weaponized Interdependence."
[23] World Bank, *Achieving Sustainable and Inclusive Artisanal and Small-Scale Mining (ASM): A Renewed Framework for World Bank Engagement* (Washington, DC: World Bank, 2024), 1–86, https://openknowledge.worldbank.org/server/api/core/bitstreams/cab95ce4-781f-42df-9c4d-912c55834c1b/content; Gavin Hilson et al., "Artisanal and Small-Scale Mining (ASM) in Sub-Saharan Africa: Reconfiguring the Sector for Sustainable Development," *Resources Policy* 66 (2020): 101622, https://doi.org/10.1016/j.resourpol.2020.101622.
[24] International Criminal Police Organization (INTERPOL), *Illicit Goods Trafficking via Port and Airport Facilities in Africa* (Lyon: INTERPOL, 2020), 47, https://enact-africa.s3.amazonaws.com/site/uploads/2020-06-29-interpol-ports-threat-assessment-report.pdf; Oguntuase Temitope Abayomi, "Nigeria's Border Porosity and Implications for National and International Security," *International Journal of Research and Innovation in Social Science* 8, no. 6 (2024): 2937–75, https://doi.org/10.47772/IJRISS.2024.806225.2020
[25] IEA, *The Role of Traceability in Critical Mineral Supply Chains*; Schöneich et al., "Traceability and Foreign Corporate Accountability in Mineral Supply Chains."
[26] Farrell and Newman, *Underground Empire* (Allen Lane, 2023); Blackwill and Harris, *War by Other Means.* Kevin D. Stringer, Madison Urban, and Andrew Mackay. "Counter Threat Finance for Strategic Competition." *The RUSI Journal* 168, no. 7 (2023): 42–51. https://doi.org/10.1080/03071847.2024.2323740.
[27] Niagalé Bagayoko, "Introduction: Hybrid Security Governance in Africa," *IDS Bulletin* 43, no. 4 (2012): 1–13, https://doi.org/10.1111/j.1759-5436.2012.00330.x; Mark Leonard, *The Age of Unpeace: How Connectivity Causes Conflict* (London: Bantam Press, 2021).

[28] Shelley, *Dirty Entanglements*; Phil Williams, *The Fifth Wave: Organized Crime in 2040* (Geneva: Global Initiative Against Transnational Organized Crime, 2024), 30, https://globalinitiative.net/wp-content/uploads/2024/11/Phil-Williams-The-fifth-wave-Organized-crime-in-2040-GI-TOC-November-2024.pdf.corruption, and terrorism now deserves high-level policy attention because of its growth trajectory. Using lively case studies, this book analyzes the transformation of crime and terrorism and the business logic of terrorism. Louise I. Shelley concludes that corruption, crime, and terrorism will remain important security challenges in the twenty-first century as a result of economic and demographic inequalities in the world, the rise of ethnic and sectarian violence, climate change, the growth of technology, and the failure of nineteenth- and twentieth-century institutions to respond to these challenges when they emerged.","editi on":"1","ISBN":"978-1-107-01564-7","license":"https://www.cambridge.org/core/terms","note":"DOI: 10.1017/CBO9781139059039","publisher":"Cambridge University Press","source":"DOI.org (Crossref

[29] Farrell and Newman, "Weaponized Interdependence."

[30] Michael Miklaucic and Jacqueline Brewer, *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington, DC: National Defense University Press, 2013), https://www.files.ethz.ch/isn/163849/convergence.pdf.

[31] Organisation for Economic Co-operation and Development, *Due Diligence Guidance for Responsible Business Conduct* (Paris: OECD, 2018), 100, https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/02/oecd-due-diligence-guidance-for-responsible-business-conduct_c669bd57/15f5f4b3-en.pdf; Organisation for Economic Co-operation and Development, *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas* (Paris: OECD, 2016).

[32] Thomas Risse, *Governance Without a State?: Policies and Politics in Areas of Limited Statehood* (Columbia University Press, 2011), https://www.jstor.org/stable/10.7312/riss15120.

[33] OECD, *Natural Resource Governance and Fragility in the Sahel*; World Bank, *Achieving Sustainable and Inclusive Artisanal and Small-Scale Mining (ASM)*.

[34] United Nations Office on Drugs and Crime (UNODC), *Trafficking in the Sahel: Guns, Gas, and Gold* (Vienna: United Nations, 2023), https://www.unodc.org/unodc/frontpage/2023/May/trafficking-in-the-sahel_-guns--gas--and-gold.html.

[35] CTED, *Concerns over the Use of Proceeds from the Exploitation, Trade, and Trafficking of Natural Resources.*

[36] Wennmann, "Economic Dimensions of Armed Groups"; Giustozzi et al., *Guns, Goods and Governance: Illicit Economies and the Foundations of Insurgent Rule*. operational costs, and economic agendas of armed groups and brings together examples from Angola, Kosovo, Sudan, Colombia, and other places. It emphasizes that information about available financing and operational costs is critical for assessing the financial and operational strength of an armed group. It also highlights the need to understand armed groups in the broader context of their evolution and the changes that organizational and territorial expansions require with regards to financing strategies. Overall, the economic dimensions of armed groups should be approached with an open mind so that issues such as financing, costs, and economic agendas can be perceived as opportunities, and not necessarily as a problem for peace.","container-title":"International Review of the Red Cross","DOI":"10.1017/S1816383111000361","ISSN":"1816-3831, 1607-5889","issue":"882","-journalAbbreviation":"Int. rev. Red Cross","language":"en","license":"https://www.cambridge.org/core/terms","page":"333-352","source":"DOI.org (Crossref

[37] Vanda Felbab-Brown, "Nonstate Armed Actors in 2023: Persistence amid Geopolitical Shuffles," *Brookings* (Washington, DC), 2023.

[38] Wennmann, "Economic Dimensions of Armed Groups."operational costs, and economic agendas of armed groups and brings together examples from Angola, Kosovo, Sudan, Colombia, and other places. It emphasizes that information about available financing and operational costs is critical for assessing the financial and operational strength of an armed group. It also highlights the need to understand armed groups in the broader context of their evolution and the changes that organizational and territorial expansions require with regards to financing strategies. Overall, the economic dimensions of armed groups should be approached with an open mind so that issues such as financing, costs, and economic agendas can be perceived as opportunities, and not necessarily as a problem for peace.","container-title":"International Review of the Red Cross","-DOI":"10.1017/S1816383111000361","ISSN":"1816-3831, 1607-5889","issue":"882","journalAbbreviation":"Int. rev. Red Cross","language":"en","license":"https://www.cambridge.org/core/terms","page":"333-352","source":"DOI.org (Crossref

[39] INTERPOL, *Illicit Goods Trafficking via Port and Airport Facilities in Africa*; Abayomi, "Nigeria's Border Porosity and Implications for National and International Security."\\uc0\\u8220{}Nigeria\\uc0\\u8217{}s Border Porosity and Implications for National and International Security.\\uc0\\u8221{}"","plainCitation":"INTERPOL, Illicit Goods Trafficking via Port and Airport Facilities in Africa; Abayomi, "Nigeria's Border Porosity and Implications for National and International Security."","noteIndex":41},"citationItems":[{"id":112,"uris":["http://zotero.org/users/local/g7SaPoqK/items/LSZSUIAD"],"itemData":{"id":112,"type":"report","event-place":"Lyon, France","language":"English","page":"47","publisher":"ENACT / INTERPOL","publisher-place":"Lyon, France","title":"Illicit Goods Trafficking via Port and Airport Facilities in Africa","URL":"https://enact-africa.s3.amazonaws.com/site/uploads/2020-06-29-interpol-ports-threat-assessment-report.pdf","author":[{"family":"INTERPOL","given":""}],"issued":{"date-parts":[["2020"]]}}},{"id":111,"uris":["http://zotero.org/users/local/g7SaPoqK/items/49GW9VL4"],"itemData":{"id":111,"type":"article-journal","abstract":"The evolution of modern borders can be traced to the partitioning of Africa during the Berlin Conference negotiations from November 15, 1884 to February 26, 1885. The artificial borders so created are accompanied with extreme porosity leading to myriads of transnational and cross-border criminalities which threatens the peace, security and stability of the region as a whole and Nigeria in particular. This study therefore seeks to examine the causes of Nigeria's border porosity, emerging cross-border related security threats, government and other stake holders efforts at curbing the menace and to interrogate the implications Nigeria's Border porosity on peacebuilding, national and international security. Talcott Parson's Theory of Functional Prerequisites served as the framework while the mixed method research design was adopted for the study. A total of eighty (80

[40] Lyes Tagziria and Lucia Bird, *Illicit Economies and Instability: Illicit Hub Mapping in West Africa 2025* (Geneva: Global Initiative Against Transnational Organized Crime, 2025), 64, https://globalinitiative.net/wp-content/uploads/2025/10/Lyes-Tagziria-Lucia-Bird-Illicit-economies-and-instability-Illicit-hub-mapping-in-West-Africa-2025-GI-TOC-October-2025.v3.pdf.

[41] World Bank, *Achieving Sustainable and Inclusive Artisanal and Small-Scale Mining (ASM): A Renewed Framework for World Bank Engagement*.

[42] UNODC, *Minerals Crime.*

[43] Yulia Krylova, *Dubai: A Global Hub for Illicit Trade and Sanctions Evasion*, Hubs of Illicit Trade Project (Fairfax, VA: Terrorism, Transnational Crime and Corruption Center, 2023), https://traccc.gmu.edu/wp-content/uploads/2024/11/Dubai-report-Updated.pdf; Simon Marks et al., "Dubai Can't Shake Off the Stain of Smuggled African Gold," *Bloomberg*, 2021.

[44] OECD, *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas*.

[45] Shelley, *Dirty Entanglements*.corruption, and terrorism now deserves high-level policy attention because of its growth trajectory. Using lively case studies, this book analyzes the transformation of crime and terrorism and the business logic of terrorism. Louise I. Shelley concludes that corruption, crime, and terrorism will remain important security challenges in the twenty-first century as a result of economic and demographic inequalities in the world, the rise of ethnic and sectarian violence, climate change, the growth of technology, and the failure of nineteenth- and twentieth-century institutions to respond to these challenges when they emerged.","edition":"1","ISBN":"978-1-107-01564-7","license":"https://www.cambridge.org/core/terms","note":"DOI: 10.1017/CBO9781139059039","publisher":"Cambridge University Press","source":"DOI.org (Crossref

[46] Financial Action Task Force, *Trade-Based Money Laundering: Trends and Developments* (Paris: FATF, 2020), 66, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf.

[47] UNODC, *Gold Trafficking in the Sahel*; Hunter, *Beyond Blood*.

[48] Marc Ummel and Yvan Schulz, *On the Trail of African Gold: Quantifying Production and Trade to Combat Illicit Flows* (Lausanne: SwissAid, 2024), 140, https://swissaid.kinsta.cloud/wp-content/uploads/2024/05/swissaid-on-the-trail-of-african-gold-web-ok.pdf.

[49] UNODC, *Gold Trafficking in the Sahel*; Krylova, *Dubai: A Global Hub for Illicit Trade and Sanctions Evasion*.

[50] Dominic Raab, *Silence Is Golden: A Report on the Exploitation of Artisanal Gold Miners to Fund War, Terrorism and Organised Crime* (London: World Gold Council, 2024), 1–50, https://www.gold.org/esg/artisanal-and-small-scale-gold-mining.

[51] Lotte Hoex et al., *The EU Conflict Minerals Regulation: High Stakes, Disappointing Results* (Brussels: European Union, 2023), 28, https://paxforpeace.nl/wp-content/uploads/sites/2/2023/10/The-EU-conflict-minerals-regulation_High-stakes-disappointing-results.pdf.

[52] CTED, *Concerns over the Use of Proceeds from the Exploitation, Trade, and Trafficking of Natural Resources.*

[53] Schöneich et al., "Traceability and Foreign Corporate Accountability in Mineral Supply Chains."
[54] Williams, *The Fifth Wave: Organized Crime in 2040*.
[55] UNODC, *Trafficking in the Sahel: Guns, Gas, and Gold*.
[1] CTED, *Concerns over the Use of Proceeds from the Exploitation, Trade, and Trafficking of Natural Resources*.

Regulatory Arbitrage and Regional Security Spillovers

Counter-Threat Finance Dynamics in Southeast Asia

By Dr. Fauzia Gustarina Cempaka Timur, Aulia Akmalina, and Alif Asy'ari

Illicit finance is a major factor in current security challenges in the Indo-Pacific. Its influence goes beyond just funding terrorism. Financial flows linked to cyber-enabled fraud, human trafficking, online gambling, and transnational organized crime increasingly operate across borders, exploiting regulatory asymmetries, uneven governance capacity, and rapid digitalization.[1] Known as regulatory arbitrage, this behavior has long been recognized in financial markets as the systematic exploitation of jurisdictional differences in rules and enforcement to minimize compliance costs or shift risk.[2] Within this regional context, Indonesia provides a relevant point of analysis due to its expanding digital financial sector and increasing regulatory efforts in counter-threat finance.

The security implications of illicit finance extend beyond material economic losses. Cyber scams cause significant harm by exploiting many people. They involve forced labor, torture, sexual violence, and extensive financial fraud. These acts violate human rights and silence journalists and civil society through intimidation

Dr. Fauzia Gustarina Cempaka Timur is an assistant professor at the Republic of Indonesia Defense University. She also serves as senior analyst in Indo-Pacific Strategic Intelligence and a subject matter expert of Political Security Pillar in localizing ASEAN Community Vision 2045. Her academic focus encompasses non-traditional security, asymmetric warfare, and societal resilience. She holds a doctorate degree in international relations. She is reachable through her email: fg.cempaka@idu.ac.id.

Aulia Akmalina is a graduate from the Asymmetric Warfare Department at the Republic of Indonesia Defense University and is currently enrolled as a project officer at the Singapore International Foundation. Her academic interests focus on the dynamics of non-conventional conflicts and the roles of non-state actors within the contemporary security landscape. She is reachable via email: aulia.akmalina@gmail.com.

Alif Asy'ari is currently a graduate student in the Asymmetric Warfare Department at the Faculty of Defense Strategy, Republic of Indonesia Defense University. His academic interests focus on asymmetric warfare, intelligence, terrorism, and insurgency with particular attention to information warfare and non-kinetic security dynamics. He is reachable via email: asyari.alif12@gmail.com.

and corruption.[3] On a wider scale, these scams disrupt national economies. They support armed groups, weaken governance, and threaten regional security. They also harm the environment and split communities, creating global effects that extend far beyond Southeast Asia.[4] In this sense, illicit finance operates as a form of indirect coercion, generating security externalities that reach beyond the financial domain itself. This change shows a broader trend in security studies. Now, non-military threats like economic disruption, cyber insecurity, and governance erosion are seen as key parts of national and regional security. In this setting, financial regulation is vital. It helps states reestablish control over international economic and digital spaces.

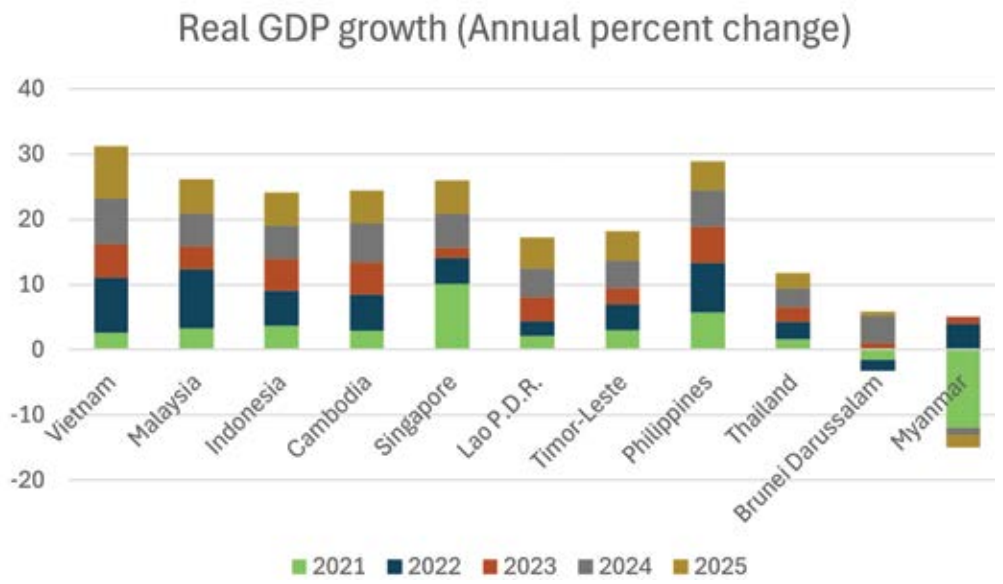
These dynamics are quite apparent in the Indo-Pacific. The region combines dense trade and financial integration, significant variation in regulatory capacity, and a rapid expansion of digital financial technologies.[5] This setup has helped cyber-scam networks and illegal finance hubs grow, especially across mainland Southeast Asia. Following the Covid-19 pandemic and political unrest in 2021, serious governance and security gaps emerged in various parts of the Mekong subregion. These conditions allowed scam centers to expand rapidly. They specialized in online fraud, crypto crimes, and investment scams referred to as "pig-butchering" schemes.[6]

The United Nations Office on Drugs and Crime (UNODC) estimates suggest these operations now cause yearly losses of up to (U.S.) $37 billion across East and Southeast Asia, underscoring both the scale of the threat and its systemic implications.[7] Scam operations differ from traditional organized crime groups by embedding themselves in global financial and payments infrastructures such as digital platforms, cross-border banking, and crypto-assets that facilitate the rapid concealment and transfer of illicit value. They turn to jurisdictions that lack strong oversight, showing how they take advantage of regulatory and governance gaps.[8] As a result, the effectiveness of national counter-threat finance policies cannot be assessed in isolation. Actions that successfully limit illegal activities in one place may cause them to shift elsewhere. This often means that illicit finance only shifted to other areas with weaker regulations rather than being fully eliminated.

Over the last decade, Indonesian authorities have actively strengthened anti-money laundering and counter-terrorism financing regulations, alongside intensifying oversight of digital financial compliance.[9] These developments are increasingly understood not only as mechanisms for promoting financial integrity but also as integral components of national security governance, aimed at reinforcing economic resilience and state authority in the face of asymmetric threats.[10] In this respect, Indonesia reflects a broader regional trajectory in which financial regulation functions as a non-kinetic instrument to disrupt transnational criminal networks operating below the threshold of armed conflict.

Amidst a changing threat landscape, Indonesia stands out as a significant economy and a key financial hub in Southeast Asia. Shown in the figure 1 above, Indonesia is among the top five Association of Southeast Asian Nations (ASEAN) member states with constant annual GDP growth. To retain the status, national authorities have actively improved regulations for anti-money laundering and counter-terrorism financing. They have also stepped-up oversight of digital financial compliance. These actions are increasingly viewed as not only mechanisms for promoting financial integrity but also as vital components of national security governance. This approach aims to bolster economic resilience and state authority in the face of asymmetric threats.[11] This perspective reveals a broader regional trend. In this case, financial regulation serves as a non-violent method to disrupt transnational criminal networks that function below the level of armed conflict.

FIGURE 1



Source: IMF Data Mapper, concluded by Authors (2026)

The effects of regulatory tightening extend far beyond national borders. In a tightly woven regional financial system, more controls in one area change cross-border incentives. Transnational financial networks adapt as enforcement pressure increases in well-regulated areas. They redirect flows, shift operations, and exploit weaknesses in governance elsewhere. This trend appears in the evolving landscape of illegal finance across mainland Southeast Asia. Scam centers and cyber fraud are increasingly emerging in regions with limited regulatory oversight.[12] To assess how effective counter-threat finance policies are, it is also important to understand both the relational and regional aspects involved.

Despite an expanding body of research on illicit finance and cyber-enabled crime in Southeast Asia, particularly studies examining the political economy of scam operations and transnational criminal networks, these analyses are frequently complemented by policy-oriented and institutional reports. These reports provide empirical mapping of evolving illicit financial ecosystems in the region, much of the focus remains on either the operational aspects of scam networks or national regulatory responses.[13] There are reports by INTERPOL Asia and South Pacific, research by Amerhauser and Thill, and also research by Sundram.[14] There is often not enough attention on how domestic counter-threat finance measures affect regional governance differences. This can lead to spillover effects across borders. Consequently, the regional security ramifications of regulatory tightening are often inadequately theorized, particularly from a relational perspective. This raises a theoretical question. Why does tighter regulation in one area create security externalities in nearby areas instead of fully dismantling illicit networks?

Conventional deterrence theory argues that when enforcement costs rise, criminal activity should decrease significantly. Studies indicate that criminal networks tend to relocate rather than completely end their operations.[15] This behavior is similar to regulatory arbitrage seen in legitimate financial markets.[16] Firms exploit jurisdictional differences to cut compliance costs. Regulatory

arbitrage theory hasn't been thoroughly examined in security studies. This is particularly true for transnational criminal networks that work across digitally connected yet politically divided regions. At the micro level, these criminal networks function as rational economic actors.

This analysis employs regulatory arbitrage theory to illustrate how domestic counter-threat finance measures lead to transnational spillovers. Originating in financial economics, regulatory arbitrage describes the systematic exploitation of differential regulatory standards across jurisdictions to minimize compliance costs or maximize operational benefits.[17] The theory often links to corporate tax avoidance and capital flows. However, it also applies to transnational criminal networks. When enforcement gets stricter in one area, smart actors look at nearby places. They move their operations to lower risk and keep market access.

Three conditions facilitate regulatory arbitrage within the Southeast Asian context. First, jurisdictional differentials create exploitable gaps. These gaps come from differences in regulatory strictness, enforcement ability, and political will in nearby areas. Indonesia's advanced financial intelligence sharply contrasts with the governance gaps in Myanmar after the coup and in Cambodia's Special Economic Zones, where oversight is limited.[18] Second, operational mobility helps scam centers tap into the Indonesian market. They rely on digital technologies such as VoIP, social media, and encrypted messaging. This access is possible even if they operate from Myanmar or Laos.[19] Third, integrated financial networks where ASEAN economic integration has built correspondent banking relationships, remittance corridors, and payment system links allow for easier cross-border fund transfers, even when networks are disrupted.[20]

In their examination of illicit drug trafficking, Windle and Farrell and Wood, et al. (2004) posited that stricter enforcement would result in spatial displacement rather than total deterrence.[21] As regulations intensify in one locality, businesses may migrate to less regulated areas within the same economic landscape. This strategic shift happens when networks pinpoint regions that enhance security and efficiency through careful analysis. Furthermore, the theory implies a notion of relational effectiveness. Policies may appear successful domestically if illicit activities diminish within national confines. However, these measures can create regional issues. They may cause activities to cluster in nearby areas with less government oversight.

Economic theories about Transnational Organized Crime (TOC) claim that these illegal groups operate like rational businesses.[22] They analyze costs and benefits to find the best locations based on regulations. Criminal networks analyze their operational choices by comparing expected returns to enforcement costs. They consider detection risks, asset seizure likelihood, and prosecution probabilities. Then, they weigh these against potential gains from market access and revenue generation.[23] If regulations increase enforcement costs too much, these networks may move to new areas. They seek places with better cost-benefit profiles, like the regulatory arbitrage seen in legitimate financial markets.[24] This optimization is not random or careless. Networks systematically assess jurisdictional differences by reviewing regulatory strictness, state enforcement capabilities, extradition risks, and available infrastructure in their operational areas. Digital technologies help create hybrid spatial strategies. They allow physical operations to move to low-enforcement areas. At the same time, businesses can still reach target populations. This is possible through encrypted communications, virtual payment systems, and social media platforms. Deciding to relocate shows an organization's strength and flexibility. Criminal enterprises often stick to established networks, even when enforcement costs increase. They typically

only change or move when regulations become too severe.[25] However, this micro-level choice happens within larger structural limits. Networks are shaped by social ties in local crime systems. They depend on access to important roles for illegal activities and the strength of connections between groups. This strengthens coordination. TOC theory highlights how displacement occurs through optimizing jurisdictional settings. It also understands that crime patterns stem from individual choices and the larger systems that shape these behaviors.

Regional Security Complex Theory (RSCT) explains why spillovers concentrate regionally rather than dispersing globally. Developed by Buzan and Wæver in 2003, RSCT posits that security dynamics cluster at regional level based on geographic proximity and interdependence where states' security problems within a region are so interlinked they cannot be analyzed separately from neighbors.[26] Four structural variables define regional security complexes: boundary (geographic delimitation), anarchic structure (multiple autonomous actors without supranational authority), polarity (distribution of power), and social construction (patterns of amity/enmity).

Southeast Asia represents a distinct regional security complex, particularly relevant to the dynamics of threat finance spillovers. Being close geographically means shorter distances for operations. This helps displaced networks reach Indonesian markets digitally while moving to areas in the Mekong subregion. ASEAN's economic collaboration has connected financial systems. It has created payment infrastructures, correspondent banking networks, and remittance channels. These links tie Indonesian financial entities to Southeast Asian economies and open up arbitrage opportunities. Governance fragmentation leads to major differences in state capacity.[27] These disparities create chances to exploit jurisdictional differences in a connected economy. ASEAN's loose structure emphasizes key principles such as sovereignty and non-interference. This approach hinders coordinated enforcement, even though member states have common security interests.[28]

RSCT predicts that security threats with transnational mobility will be found mainly in regional security complexes, rather than spread out globally. This is due to being close geographically, will reduce costs, and regional economic integration provides the necessary infrastructure. It also predicts that failures to coordinate are due to the basic structure of governance, which is anarchic, rather than just a lack of political will. To respond effectively, institutions are needed that can overcome the limits of sovereignty, but ASEAN's structure does not provide these.[29]

These theoretical perspectives are complementary rather than competitive. Regulatory arbitrage theory explains how stronger enforcement in Indonesia causes displacement of the scammer cells. Different laws create reasons for people to move. RSCT shows the spatial pattern of spillovers. These perpetrators mainly focus on mainland Southeast Asia. This happens due to nearby connections and divided governance. These theories provide a clear view: regulatory tightening creates arbitrage incentives. Then, networks exploit these within Southeast Asia's security framework. This leads to ongoing spillovers because ASEAN's anarchic structure makes coordinated responses hard.

Accordingly, this study examines the regional security implications of domestic counter-threat finance measures for cross-border illicit financial flows in the Indo-Pacific. It advances three core contributions. First, by conceptualizing financial regulation as a form of asymmetric security governance. Second, by demonstrating that policy effectiveness is relational rather than purely national. And third, by situating these dynamics within the political economy of mainland Southeast Asia. Indonesia is employed as a focal case through which these dynamics can be examined, given its

combination of regulatory tightening, financial system significance, and exposure to cross-border illicit financial flows within the regional system. The analysis proceeds through a qualitative examination of regulatory practices and regional security dynamics, before considering their broader theoretical and policy implications.

The analysis proceeds from the premise that transnational criminal networks operate with a strategic logic comparable to legitimate market actors, systematically evaluating regulatory environments and reallocating activities to optimize trade-offs between security and efficiency. Utilizing regulatory arbitrage theory, this study posits that the intensification of enforcement in Indonesia as the focal case engenders jurisdictional differentials, which in turn incentivize a spatial shift towards regulatory peripheries. Furthermore, drawing on RSCT, this research shows that spillover effects cluster by region. Southeast Asia is defined by geographic proximity, financial system integration, and governance fragmentation. These traits create conditions that help arbitrage while they also limit coordinated responses.

Methodology

This study adopts a qualitative research design grounded in interpretive policy analysis to examine how domestic counter-threat finance measures generate regional security spillovers within the Indo-Pacific. Rather than assessing policy effectiveness through quantitative indicators, the analysis focuses on how regulatory tightening reshapes incentives, practices, and the spatial organization of illicit financial networks across borders. This approach is appropriate for the research question, as the dynamics of threat finance and displacement are embedded in regulatory interactions, institutional contexts, and political economy conditions that cannot be adequately captured through single-country or purely statistical analysis.

The analysis draws on qualitative data derived from regulatory documents, official policy materials, and authoritative secondary sources published between 2020 and 2025. Primary materials include national frameworks, policy statements, and supervisory documents related to anti-money laundering, counter-terrorism financing, and digital financial governance. These sources are complemented by regional security and threat finance reports produced by international and regional organizations, which provide detailed accounts of illicit financial practices, cyber-enabled fraud, and the organization of scam networks across mainland Southeast Asia.

Analytically, the study proceeds in three stages. First, counter-threat finance regulations are examined to identify their underlying security rationales and enforcement logics. Second, regional empirical materials are analyzed to trace patterns of adaptation and displacement in illicit financial practices following regulatory tightening. Third, these findings are synthesized through a cross-level analysis linking domestic regulatory actions to regional security outcomes. This stepwise procedure ensures analytical transparency and allows the analysis to be conceptually replicated in other regions characterized by similar regulatory asymmetries and governance conditions.

Several limitations should be acknowledged. The study relies on document-based qualitative materials and does not incorporate primary fieldwork or transaction-level data, which could further illuminate network-level adaptations. Many of the sources for theoretical context are older than ten years old, and although for now it is seemingly relevant, newer refinement and constantly revisited data sources might be needed to validate some of the points made in this paper. Future research could address these gaps through mixed method approaches or comparative analysis across regions with different governance architectures. More broadly, the findings suggest that counter–threat finance in the Indo-Pacific cannot

be addressed through unilateral regulatory strategies alone. As financial systems become increasingly interconnected, financial security must be reconceptualized as a shared regional concern, shaped by coordination, information exchange, and collective governance rather than isolated national interventions.

Results and Discussion: Domestic Regulatory Tightening as the Securitization of Financial Governance

Since 2020, Indonesia has updated its counter-threat finance regulations. This serves as a real-world case to test what regulatory arbitrage theory predicts. Indonesia strengthened its domestic oversight. At the same time, neighboring regions had weaker regulations. This created a gap in regulatory stringency, leading to arbitrage opportunities. Recognizing the size of these differentials helps explain later spatial displacement patterns.[30]

From a regulatory arbitrage perspective, as conceptualized in studies of how actors exploit differences in regulatory environments, Indonesia's measures increased three types of enforcement costs for illicit networks: (1) detection risk through enhanced financial intelligence capabilities and data integration, (2) operational costs via stricter KYC requirements and beneficial ownership transparency, and (3) asset seizure risk through expanded confiscation powers and inter-agency coordination.[31] These measures changed Indonesia from a lenient place to a high-risk area for scam centers and money laundering. This shift pushed many operations to relocate to stay viable.[32]

The analysis shows a clear trend of stricter regulations in counter-threat finance. This involves greater supervisory authority, stricter compliance rules, and a more thorough review of financial activities. These measures have shifted from just ensuring financial integrity. They now represent a regulatory approach that treats illicit finance as a risk to economic stability and state power.

In the Indonesian context, this shift became particularly visible during 2023–2024, when the Anti–Money Laundering Law (Law No. 8/2010) was put into use more boldly following a period in which enforcement remained relatively fragmented and reactive. However, it intensified as the rapid expansion of cyber-enabled fraud and online gambling after the COVID-19 period elevated illicit finance into a priority security concern to target the financial systems backing online gambling. It did this mostly through required reporting, transaction monitoring, and large-scale account blocking. Comparative research on online gambling laws shows a shift in anti-money laundering (AML) strategies. In various regions, these frameworks are moving away from simple compliance. Instead, they are becoming tools that actively limit market activities.[33]

Indonesian legal analyses indicate that financial enforcement developed because prohibitive and punitive measures alone were not effective in curbing online gambling.[34] These developments highlight how counter–threat finance connects financial oversight with security goals. It emphasizes enforcement, coordination among agencies, and regulatory integration. This shift shows its role as a governance tool, not just a narrow compliance system.

Scam operations thrive due to unmet demand and weak regulations in the digital space. Strong economic gains for both perpetrators and facilitators still last despite the pressure of enforcement. In Indonesia, large victim payouts encourage more people to join scam operations. This trend stems from poverty and high youth unemployment in their countries. This scenario engenders a self-reinforcing cycle that national-level interventions struggle to disrupt independently. Current Indonesian laws struggle with accessibility and enforcement. Regulations are fragmented among the Financial Services Authority, the Ministry of Communication and Digital Affairs, and the Indonesian National Police. This leads to a lack of

cohesive extraterritorial jurisdiction. Public education initiatives are mostly reactive. They often fail to reshape how society sees risks.

As operations shift online, regulation weakens. Scams on foreign servers slip past takedown requests. Cryptocurrency transactions avoid banking oversight. Meanwhile, AI-generated deepfakes boost impersonation tactics, making detection more difficult.[35] This digital shift creates more arbitrage opportunities. Networks are forming in areas with little governance, like Myanmar's Kokang region.[36] At the same time, they are also reaching Indonesian audiences from a distance. As a result, this change turns what might look like national success into a regional expansion. It lacks any supranational systems to bridge the gap in rules.

This regulatory trajectory constitutes an empirical finding rather than a normative claim. Financial regulation has shifted from a neutral tool to an active strategy. It now aims to disrupt global illegal networks that function below the level of armed conflict. The domestic regulatory environment raises transaction costs. It also makes it harder to access formal financial channels.

Plus, it increases the visibility of illegal financial practices in regulated systems. Regulatory tightening is strong in digital finance and crypto activities. Authorities aim to balance financial innovation with increased security concerns. The analysis reveals that tougher licensing requirements, improved customer due diligence, and increased transaction monitoring have significantly limited anonymity on regulated platforms. These measures are often seen as needed to tackle risks from cyber fraud, online gambling, and money laundering. This is especially true in digital financial systems.

The enforcement logic behind these measures focuses on deterring crime in formal financial systems. It does not aim to fully eliminate illicit finance. As compliance requirements grow tougher, illegal actors deal with increased costs and greater risks. This drives them to seek alternative paths beyond regulated spaces. This pattern suggests that success in domestic regulation is conditional. It creates responses that reach beyond national borders and alter the regional threat landscape.[37]

Regulatory Arbitrage and Spatial Displacement Resulting in Regional Spillover Dynamics

The spatial reconfiguration of illicit finance across mainland Southeast Asia following Indonesian enforcement intensification exemplifies regulatory arbitrage dynamics operating at regional scale. As predicted by arbitrage theory, transnational criminal networks reacted to wider jurisdictional gaps not by halting their activities but by moving to less regulated areas. This change boosts their security and improves their economic efficiency.[38]

This relocation follows identifiable patterns consistent with theoretical expectations. First, networks evaluate potential host jurisdictions in the regional security complex. They check factors such as regulatory strictness, state enforcement, political stability, and extradition risk. Then they move to places with weak regulations. These areas also have support systems like telecommunications, finance, and transportation. Third, networks centralize their operations in specific areas. This limits their exposure and helps them function efficiently. Lastly, they ensure the digital technologies such as VoIP, social media, encrypted messaging, and cryptocurrency to enable networks to reach Indonesian victims remotely, even when they relocate.[39]

Figure 1 offers distributional data that is broadly consistent with the spatial clustering predicted by regulatory arbitrage theory, though the pattern warrants careful interpretation and does not, in itself, constitute confirmation of the mechanism. This supports the spatial clustering arbitrage theory. Transnational networks take

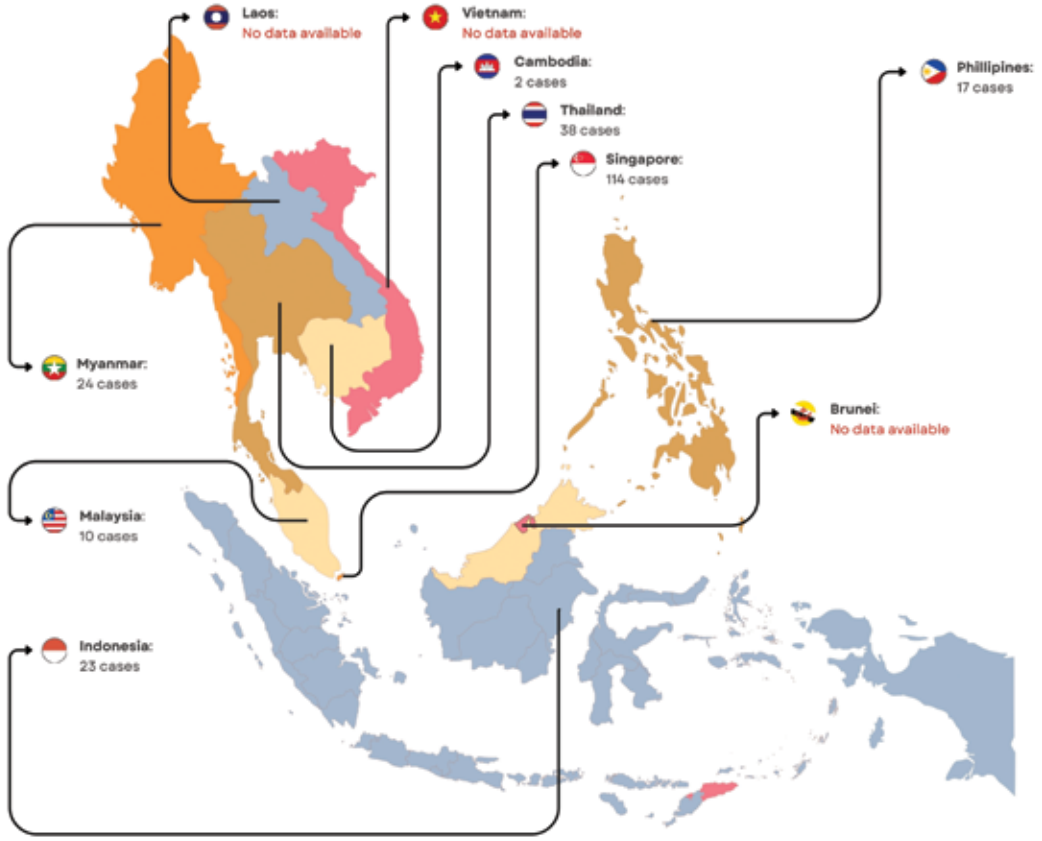
advantage of differences in laws, focusing their activities in areas with less oversight.[40] The concentration of counter-threat finance enforcement cases across Southeast Asia, with Singapore registering 114, Thailand 38, Myanmar 24, Indonesia 23, Malaysia 10, and Cambodia 2. This is suggestive of a dynamic in which jurisdictions with stronger institutional capacity surface more cases, while those facing governance deficits record fewer detections, not necessarily because illicit activity is absent but because the infrastructure required to identify, investigate, and prosecute such activity remains constrained.[41]

Several limitations qualify this reading and prevent a straightforward causal inference from these figures. First, and most critically, enforcement case counts are a function of detection capacity and reporting practice, not a direct index of underlying threat levels. Singapore's high case count may paradoxically reflect the superior performance of its financial intelligence infrastructure rather than a disproportionate concentration of criminal networks; inversely, Cambodia's two cases almost certainly reflect acute under-detection rather than low criminal presence. This shows a distinction the available data cannot cleanly resolve. Second, the study relies on UNODC-compiled data for cross-jurisdictional comparison, a source that, while authoritative, introduces classification variance and comparability constraints given that reporting standards, definitional frameworks, and institutional reporting cultures differ considerably across member states. Third, the 2018–2023 data window encompasses a period of exceptional structural disruption: the COVID-19 pandemic reorganized illicit financial flows throughout the region, while the 2021 Myanmar military coup created acute governance ruptures that may account for shifts in the data independently of regulatory arbitrage dynamics. These caveats do not undermine the plausibility of the arbitrage interpretation; rather, they establish that the distributional pattern is consistent with the theoretical expectation of spatial clustering. No stronger claim should be advanced on the basis of this data alone. Networks compare regulatory environments to lower compliance costs and oversight risks while maintaining market access. Indonesia's 23 cases showed increased regulatory tightening. This didn't remove threats; instead, it caused geographic displacement.

Thailand's 38 cases represent the predicted "sweet spot"—weaker than Singapore, yet stronger than Myanmar and Cambodia. Rather than selecting the weakest jurisdictions, transnational criminal organizations tend to optimize trade-offs between low enforcement risk and operational viability. While Myanmar and parts of Cambodia offer weaker regulatory oversight, they also present higher levels of instability, infrastructural limitations, and operational uncertainty. Networks targeting Indonesian victims have relocated to Thailand and Myanmar. However, they maintain access through digital infrastructure and cross-border financial corridors. Indonesia's success in enforcing laws relates more to where actions happen than to removing threats. This reflects a pattern where local regulations create regional effects. It explains why national counter-threat finance methods often struggle in related security areas. This highlights the difficulties in tackling these connected threats.

A notable example of these spillover dynamics is the emergence of large-scale scam centers that operate as integrated illicit enterprises. These centers differ from scattered or chance criminal acts. They work as organized hubs. They mix cyber fraud, forced labor, and money laundering into one system. Investigations show that scam operations are usually set up in economic zones with loose rules or in areas where the state has little control. This allows them to exploit victims and use digital deception methods.[42] This consolidation of illegal

Figure 2. Counter-Threat Finance Disparities Across Southeast Asia.



Sources: Authors' own work and UNODC (2018-2023).

activities signals a major change in illicit finance. It shifts from scattered criminal actions to more centralized and resilient networks.

These consolidated operations continue to thrive due to adaptable financial flows. They capitalize on the regulatory differences found in different jurisdictions. Scam money is increasingly funneled through complicated paths. It involves banks, payment services, and digital assets. This makes it easy to move and hide funds quickly. Studies on money laundering today reveal that uneven regulations let criminals take advantage of weak oversight. They move transactions from tightly regulated systems to offshore or lightly controlled intermediaries.[43] This adaptive use of financial systems makes illicit networks more resilient, despite increased enforcement efforts.

These findings indicate that domestic actions against financial threats have worked well. They have strengthened regulatory control in formal financial systems. However, the effectiveness of these measures is context dependent. Regulatory tightening raises compliance costs and enforcement pressure in well-regulated areas. This change affects how illicit financial networks operate. It doesn't eliminate them entirely but reshapes their environment. As a result, processes of relocation, consolidation, and financial adaptation redistribute risk across the region by following existing governance asymmetries. This situation highlights how

fragmented financial governance affects regional security. It sets the stage for exploring the limits of unilateral regulatory methods in the next section.

Regional Security Complex Theory explains why spillovers are more likely to occur in mainland Southeast Asia than in other weak-governance zones, such as West Africa, Central America, or Pacific Island states. Three factors contribute to this regional clustering:

- **Geographic Proximity and Operational Distance**. The Mekong subregion is near Indonesia's financial network. This closeness cuts costs for maintaining market access. Networks that relocate to Myanmar, Cambodia, or Laos can target Indonesian victims digitally with minimal latency. Furthermore, using trafficked Indonesian workers helps reduce language barriers. At the same time, it cuts down on financial transfer distances. In contrast, more distant jurisdictions lack these advantages.[44]
- **Financial System Integration via ASEAN Economic Community**. Regional economic integration has formed an interconnected financial system. It connects Indonesia's payment infrastructure, correspondent banking, and remittance channels with those in mainland Southeast Asia. This integration allows displaced networks to still access Indonesian banking for money laundering, even if they have relocated. The economic framework that helps legal trade also opens doors for illegal fund transfers.[45]
- **Governance Fragmentation within Integrated Economic Space**. The regional security complex varies greatly in state capacity. For example, Singapore and Indonesia boast strong regulatory systems and enforcement. Meanwhile, Myanmar, Cambodia, and Laos face serious governance challenges. This disparity results in differing oversight across a regionally integrated financial space. This is a significant issue for threat finance. In regions such as West Africa or Central America, there are weak-governance states. Yet, they lack the financial ties to target-rich areas like Indonesia.[46]

RSCT's notion of anarchic structure highlights how various independent actors' function without a higher authority.[47] This sheds light on why coordination failures persist, even when there are common interests. ASEAN's key principles include sovereignty, non-interference, and consensus. These principles hinder coordination at a supranational level, which is needed to handle jurisdictional differences.[48] Even when countries impacted by spillover acknowledge the issue, ASEAN can't enforce rules or cooperation without everyone's consent. This challenge comes from the region's social dynamics, not only a lack of political will.

This result supports the main idea of regulatory arbitrage theory. It shows that tightening rules in one country only moves the problem elsewhere. This happens without coordinating regional enforcement to reduce the gaps between different laws. The policy in Indonesia has led to fewer scam centers. But this success has a downside: it pushes operations to nearby regions with weak governance. These areas then target Indonesian victims remotely. From a national security perspective, Indonesia was able to move the threat outside its borders. The threat still exists from a regional security standpoint. It could be getting worse as organizations merge in unregulated areas.[49]

Limits of Unilateral Regulation and Regional Security Implications

The spillover dynamics discussed above point to a structural limitation in the way counter-threat finance measures are currently conceived and implemented. Although domestic regulatory tightening may enhance national resilience, its

effectiveness is constrained by the absence of regionally harmonized governance mechanisms. Analyses of regional security governance have long noted that transnational threats operating below the threshold of armed conflict tend to exploit precisely such coordination gaps, where jurisdictional boundaries fragment regulatory authority and dilute enforcement capacity.[50] In the context of illicit finance, this fragmentation enables criminal networks to treat regulatory diversity as an opportunity rather than a constraint.

These limitations become particularly evident when counter-threat finance is pursued primarily through unilateral or nationally anchored regulatory strategies. While such approaches may succeed in tightening oversight within individual jurisdictions, they rarely address the cross-border mobility of illicit financial networks. In the absence of mechanisms for shared intelligence, coordinated supervision, and mutual enforcement, regulatory disparities persist and are actively leveraged by transnational actors. This dynamic reinforces a pattern in which security externalities are displaced rather than resolved, allowing regional vulnerabilities to deepen even as national controls improve.[51]

From a broader Indo-Pacific security perspective, the implications of these findings extend beyond illicit finance as a discrete policy domain. Financial regulation increasingly functions as a non-kinetic instrument of security governance, yet its effectiveness remains contingent on the alignment of regulatory practices across interconnected systems. Where coordination remains weak, as reflected in the largely voluntary and consensus-based character of existing regional cooperation frameworks, counter–threat finance measures risk producing uneven security outcomes that undermine collective resilience. In such settings, regulatory divergence does not merely limit enforcement capacity but actively shapes the distribution of security risks across the region.[52]

Taken together, these observations indicate that counter–threat finance in the Indo-Pacific cannot be effectively understood (or governed), through a purely national lens. The persistence of spillovers reflects not only the adaptive behavior of transnational illicit networks, but also the structural constraints of regional governance architectures that prioritize sovereignty over integration. Institutional analyses suggest that such configurations tend to favor flexibility at the expense of enforcement coherence, creating durable spaces in which illicit financial activity can relocate, consolidate, and endure across borders. Addressing these dynamics therefore requires a reconceptualization of financial security as a shared regional concern, rather than as an aggregation of nationally bounded regulatory efforts.[53]

Conclusion

This article has examined the regional security implications of domestic counter-threat finance measures in the Indo-Pacific, focusing on how stricter regulations affect cross-border illicit financial activities. The analysis shows that stronger financial regulation helps control and resilience in domestic systems. However, its effectiveness relies on how these systems relate to each other. Regulatory pressure does not eliminate illicit finance. It shifts incentives and arrangements instead. As a result, transnational networks adapt and exploit varying governance across the region. As a result, counter-threat finance works more as a driver of change in the system than as a way to contain the problem.

This study reconceptualizes financial regulation as a governance instrument with security consequences that extend well beyond its conventional framing as a compliance mechanism. Rather than treating anti-money laundering and counter-terrorism financing measures as technical

obligations or procedural requirements, the analysis demonstrates that regulatory tightening produces spatial and structural effects on illicit financial networks that carry strategic significance—analogous, in non-kinetic terms, to the displacement effects typically associated with more direct forms of security intervention. In this sense, regulatory power constitutes one component of a broader security toolkit, to be deployed alongside diplomatic coordination, intelligence sharing, law enforcement cooperation, and institutional capacity building. It is not a self-sufficient instrument, and the present findings caution against treating it as such.

Furthermore, because the security effects of regulation are relational, spilling across borders along patterns shaped by governance asymmetries, the capacity-building challenge is not merely national but regional in scope. In the ASEAN context, where consensus-based governance constrains supranational enforcement authority, this suggests that bilateral and sub-regional capacity partnerships—particularly between higher-capacity jurisdictions such as Singapore and Indonesia and lower-capacity Mekong states—may represent the most operationally realistic pathway to narrowing the governance gaps that arbitrage dynamics exploit. Regulatory power, to function as a genuine security instrument, must ultimately be embedded within a coordinated regional framework in which implementation capacity is harmonized.

Endnotes

[1] United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia* (Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, April 2025), https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.
[2] Frank Partnoy, "Financial Derivatives and the Costs of Regulatory Arbitrage," *Journal of Corporation Law* 22 (1997): 211–56, https://lawcat.berkeley.edu/record/1116087/files/fulltext.pdf.
[3] Global Initiative Against Transnational Organized Crime (GI-TOC), *Compound Crime: Cyber Scam Operations in Southeast Asia* (Geneva: Global Initiative Against Transnational Organized Crime, May 2025), https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.
[4] GI-TOC, *Compound Crime: Cyber Scam Operations in Southeast Asia.*
[5] Financial Action Task Force (FATF), *Anti-money Laundering and Counter-Terrorist Financing Measures: Indonesia—Fourth Round Mutual Evaluation Report* (Paris: FATF, 2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.
[6] UNODC, *Inflection Point,* 7-15.
[7] UNODC, *Inflection Point,* 25-26.
[8] David AldamaNavarrete, "Dark Banking? Banks and Illicit Deposit Flows" (SSRN Working Paper, March 24, 2021), https://doi.org/10.2139/ssrn.3811752.
[9] Fauzia Gustarina Cempaka Timur and Yanyan M. Yani, "Facing ISIS Returning Foreign Terrorist Fighters: Indonesia Perspective," Jurnal Pertahanan no. 2 (2019), https://doi.org/10.33172/jp.v5i2.553.
[10] FATF, *Anti-money Laundering and Counter-Terrorist Financing Measures: Indonesia—Fourth Round Mutual Evaluation Report*.
[11] GI-TOC, *Compound Crime: Cyber Scam Operations in Southeast Asia.*
[12] GI-TOC, *Compound Crime: Cyber Scam Operations in Southeast Asia*.
[13] Ivan Franceschini, Ling Li, and Mark Bo, "Compound Capitalism: A Political Economy of Southeast Asia's Online Scam Operations," *Critical Asian Studies* 55, no. 4 (2023): 575–603, https://doi.org/10.1080/14672715.2023.2268104. ; GI-TOC, *Compound Crime: Cyber Scam Operations in Southeast Asia.*
[14] INTERPOL, *Interpol Asia and South Pacific Cyber Threat Assessment* (Singapore: Interpol, 2026), https://www.interpol.int/content/download/24327/file/CYBER_ASP%20Cyber%20Threat%20Assessment%20Report_2025_2026_v4.pdf; Kristina Amerhauser and Audrey Thill, *The Business of Exploitation, the Economics of Cyber Scam Operations in Southeast Asia* (Global Initiative against Transnational Organized Crime). https://globalinitiative.net/analysis/cyber-scam-operations-south-east-asia/.; Pushpanathan Sundram, "ASEAN cooperation to combat transnational crime: progress, perils and prospects", *Front. Polit. Sci.6:1304828.* https://doi.org/10.3389/fpos.2024.1304828. ; Franceschini et al., 576.
[15] James Windle and Graham Farrell, "Popping the Balloon Effect: Assessing Drug Law Enforcement in Terms of Displacement, Diffusion, and the Containment Hypothesis," *Substance Use & Misuse* 47, no. 8–9 (2012): 868–76, https://doi.org/10.3109/10826084.2012.663274.
[16] Partnoy, "Financial Derivatives and the Costs of Regulatory Arbitrage."
[17] Partnoy, "Financial Derivatives and the Costs of Regulatory Arbitrage," 215–20.
[18] GI-TOC, *Compound Crime: Cyber Scam Operations in Southeast Asia*, 8–15.
[19] UNODC, *Inflection Point*, 27–31.
[20] FATF, *Anti-money Laundering and Counter-Terrorist Financing Measures: Indonesia—Fourth Round Mutual Evaluation Report,* 30-34.
[21] Evan Wood et al., "Displacement of Canada's Largest Public Illicit Drug Market in Response to a Police Crackdown," *CMAJ* 170, no. 10 (2004): 1551–56, https://doi.org/10.1503/cmaj.1031928.
[22] Peter Reuter, *Disorganized Crime: The Economics of the Visible Hand* (Cambridge, MA: MIT Press, 1983).
[23] Phil Williams, "Transnational Organized Crime and the State," in *The Emergence of Private Authority in Global Governance*, ed. Rodney Bruce Hall and Thomas J. Biersteker (Cambridge: Cambridge University Press, 2002), 161–82, https://doi.org/10.1017/CBO9780511491238.
[24] Partnoy, "Financial Derivatives and the Costs of Regulatory Arbitrage."
[25] Casper van Elteren, Vítor V. Vasconcelos, and Mike Lees, "Criminal Organizations Exhibit Hysteresis, Resilience, and Robustness by Balancing Security and Efficiency," *Scientific Reports* 14, no. 1 (2024): 17678, https://doi.org/10.1038/s41598-024-68445-0.
[26] Buzan, Barry and Ole Wæver, *Regions and Powers: The Structure of International Security* (Cambridge: Cambridge University Press, 2003), 44.

[27] Alexei Gloukhovtsev, John W. Schouten and Pekka Mattila, "Toward a General Theory of Regulatory Arbitrage: A Marketing Systems Perspective," *Journal of Public Policy & Marketing* 37, no. 1 (2018): 142–151, https://doi.org/10.1509/jppm.16.0178.
[28] Amitav Acharya, *Constructing a Security Community in Southeast Asia: ASEAN and the Problem of Regional Order*, 2nd ed. (London: Routledge, 2009).
[29] Buzan and Wæver, *Regions and Powers*, 40–46.
[30] FATF, *Anti-money Laundering and Counter-Terrorist Financing Measures,* 10–18.
[31] Gloukhovtsev, Schouten and Matilla, "*Toward a General Theory of Regulatory Arbitrage.*"
[32] Republic of Indonesia, Law No. 8 of 2010 Concerning the Prevention and Eradication of the Criminal Act of Money Laundering, State Gazette of the Republic of Indonesia Year 2010 No. 122.
[33] Slobodan Tomic, "Regulatory Approach to Anti-Money Laundering in Online Gambling in the UK," in *Financial Technology and the Law: Combating Financial Crime*, ed. Doron Goldbarsht and Louis de Koker (Cham: Springer, 2022), 47–65, https://doi.org/10.1007/978-3-030-88036-1_3.
[34] Siti Farhani et al., "Pengaturan Tindak Pidana Judi Online Menurut Sistem Hukum Ekonomi dan Teknologi di Indonesia," *Begawan Abioso* 16, no. 2 (2025): 75–83.
[35] Azfer A. Khan, "Reconceptualizing Policing for Cybercrime: Perspectives from Singapore," *Laws* 13, no. 4 (2024): 44, https://doi.org/10.3390/laws13040044.
[36] GI-TOC, *Compound Crime: Cyber Scam Operations in Southeast Asia*.
[37] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.
[38] UNODC, *Inflection Point*, 16–24.
[39] Malm, Aili E. and Gisela Bichler, "Why Networks?," in *Disrupting Criminal Networks: Network Analysis in Crime Prevention,* ed. Aili E. Malm and Gisela Bichler (Boulder, CO, and London: FirstForumPress, 2015), 1–8, https://doi.org/10.13140/2.1.5030.3682.
[40] van Elteren, Vasconcelos, and Lees, Mike. "Criminal Organizations Exhibit Hysteresis, Resilience, and Robustness by Balancing Security and Efficiency." Criminal organizations exhibit hysteresis, resilience, and robustness by balancing security and efficiency. Sci Rep 14, 17678 (2024). https://doi.org/10.1038/s41598-024-68445-0.
[41] This data is rendered from UNODC official data sources, filtered and calculated by authors, 2018-2023. United Nations Office on Drugs and Crime (UNODC), "Data Portal: Economic and Corruption Data," accessed [January 2026] https://data.unodc.org/datareport/econ-corruption.
[42] UNODC, *Inflection Point*, 10–20.
[43] AldamaNavarrete, "Dark Banking? Banks and Illicit Deposit Flows." (paper presented at the American Economic Association Annual Meeting, January 3–5, 2021), https://www.aeaweb.org/conference/2021/preliminary/paper/KEfrtZRS.
[44] GI-TOC, *Compound Crime: Cyber Scam Operations in Southeast Asia*.
[45] FATF, *Anti-money Laundering and Counter-Terrorist Financing Measures,* 30-34.
[46] UNODC, *Inflection Point*, 16–24.
[47] Barry Buzan and Ole Wæver, *Regions and Powers,* 40–46.
[48] Acharya, *Constructing a Security Community in Southeast Asia*.
[49] Partnoy, "Financial Derivatives and the Costs of Regulatory Arbitrage."
[50] Williams, "Transnational Organized Crime and the State".
[51] Acharya, *Constructing a Security Community in Southeast Asia*.
[52] Acharya, *Constructing a Security Community in Southeast Asia.*
[53] Williams, "Transnational Organized Crime and the State."

Can the Weak Resist the Strong?

Venezuela's Hybrid Asymmetric Options Against U.S. Coercion

By Jithin Raveendran

Introduction

In the evolving landscape of great-power competition, weak and isolated states increasingly rely on hybrid and asymmetric strategies to resist coercion from militarily superior adversaries. Venezuela represents a prominent example of this dynamic. For much of the past decade, the Venezuelan state faced comprehensive United States economic sanctions, financial isolation, and recurrent military signalling in the Caribbean.[1] In response, Caracas developed a survival-oriented defence posture combining irregular capabilities, informational operations, proxy networks, and external partnerships with Russia, Iran, and China. This article investigates how a conventionally weak, resource-dependent state attempts to employ hybrid asymmetry to complicate, delay, or politically disincentivize coercive pressure from a stronger opponent.

However, the strategic assumptions underlying this posture were dramatically tested by "Operation Absolute Resolve" (2026), a rapid United States operation that captured President Nicolás Maduro and demonstrated the vulnerability of Venezuela's centralized command structure to precision intelligence-driven intervention.[2] The operation revealed the limits of Venezuela's existing deterrence posture and highlighted the persistent structural imbalance between technologically advanced expeditionary powers and weaker states relying on hybrid resistance strategies. At the same time, the episode illustrates a broader strategic puzzle: even when conventional deterrence fails, weaker states often continue to rely on asymmetric methods designed not to defeat a stronger adversary, but to raise the operational, political, and reputational costs of intervention.

This study argues that Venezuela's resistance strategy reflects what this article terms deterrence of inconvenience. Rather than attempting to defeat the United States militarily or prevent intervention outright, the Venezuelan state has pursued a strategy aimed at generating friction across multiple domains—maritime,

Jithin Raveendran is a Doctoral Candidate in the Department of International Relations and Politics at the Central University of Kerala, India. His ongoing research critically examines Russia's counterterrorism efforts, both within its borders and in international contexts, focusing on their evolution, strategic implications, and global engagements.

informational, proxy, and diplomatic—to complicate escalation and raise the political and operational costs of coercive action. Deterrence of inconvenience operates by multiplying disruptions rather than denying access or threatening overwhelming retaliation. Its objective is not decisive deterrence, but the creation of persistent uncertainty and operational inconvenience for the stronger adversary.

The research employs a qualitative, theory-informed case study grounded in the literatures on asymmetric conflict, hybrid warfare, and deterrence theory. These fields are synthesized to conceptualize deterrence of inconvenience as a coherent resistance model through which weak states exploit the structural, informational, and psychological vulnerabilities of stronger adversaries. Data are drawn exclusively from open-source materials, including defence analyses, declassified reports, academic publications, and verified media sources between 2019 and 2026. The study employs process tracing to establish linkages between U.S. coercive actions including sanctions, naval deployments, and targeted operations and Venezuelan hybrid responses.

Several limitations constrain the scope and generalizability of the findings. First, the covert nature of hybrid operations limits access to verifiable data on command-and-control relationships, particularly regarding proxy and paramilitary networks. Second, the measurement of deterrence effects especially political and informational costs relies on inferential indicators such as behavioural adjustments, signalling shifts, and operational posture changes by the United States. Third, the analysis remains sensitive to ongoing developments following "Operation Absolute Resolve," which may further reshape Venezuela's strategic posture.

Despite these constraints, the Venezuelan case offers a revealing lens through which to examine a broader transformation in contemporary deterrence. As technological diffusion and hybrid tactics expand the strategic toolkit available to weaker actors, deterrence increasingly operates through disruption rather than parity. The Venezuelan experience suggests that weaker states may attempt to survive the pressure of stronger adversaries not by preventing intervention outright, but by multiplying the inconveniences associated with coercion.

Classical Deterrence: Denial and Punishment

Deterrence has traditionally been understood through two primary mechanisms: deterrence by punishment and deterrence by denial. Classical deterrence theory, developed during the Cold War, defines deterrence as the use of threats to prevent an adversary from taking an undesirable action by shaping their expectations about the costs and likelihood of success of aggression.[3] Within this framework, deterrence by punishment seeks to prevent hostile action by threatening severe retaliation after aggression occurs. If an adversary believes that an attack will trigger unacceptable damage, whether military, economic, or political they may decide that the costs outweigh any potential gains.[4] Deterrence by denial, by contrast, attempts to discourage aggression by convincing the adversary that an attack will fail because defensive capabilities can prevent the attacker from achieving their objectives.[5] Rather than relying on retaliation, denial seeks to undermine the perceived feasibility of successful aggression through strong defensive posture, territorial protection, and resilience against attack.

Both forms of deterrence assume that the defending state possesses sufficient military capability and institutional stability to either retaliate effectively or deny access to the aggressor. However, weaker states confronting overwhelming military asymmetry may lack the resources necessary to sustain either credible punishment or robust denial against a technologically superior adversary. In such

cases, alternative forms of deterrence may emerge that rely less on military parity and more on the ability to generate operational friction and political complications for the aggressor. It is within this context that this article conceptualizes deterrence of inconvenience as a hybrid adaptation of classical deterrence logic.

This form of deterrence emerges primarily in contexts of extreme power asymmetry, where weaker states lack the military capacity to impose decisive punishment or to deny access to a superior force. Instead, they attempt to influence the adversary's strategic calculus by introducing dispersed forms of resistance that increase uncertainty and prolong operational timelines. Deterrence of inconvenience therefore functions less as a mechanism for preventing conflict than as a strategy for complicating it. By multiplying small but persistent obstacles across military, political, and informational domains, the weaker actor seeks to transform intervention from a rapid coercive action into a prolonged and politically sensitive undertaking. In this sense, the strategy reflects an adaptation of deterrence logic under conditions where conventional military parity is unattainable.

Deterrence of Inconvenience: Distributed Deterrence in the Hybrid Domain

The concept of deterrence of inconvenience rests on the strategic logic of distributed disruption across multiple domains. When a materially weaker actor confronts a far stronger adversary, conventional victory is rarely achievable. Instead, the weaker actor seeks to influence the strategic calculus of the stronger power by raising the operational, political, and reputational costs associated with intervention. Deterrence of inconvenience therefore operates through what this study describes as distributed deterrence, a mechanism in which deterrent effects are generated through dispersed forms of friction rather than centralized military strength.

This logic builds on scholarship examining how weaker actors can influence stronger opponents by forcing them into politically costly or strategically constrained responses. Rather than mirroring the military capabilities of the stronger adversary, the weaker actor exploits asymmetries in political sensitivity, information environments, and the operational rigidity of large conventional forces. By dispersing resistance across multiple domains, the weaker actor seeks to create cumulative costs that alter the decision-making calculus of the stronger power.

The contemporary security environment facilitates this approach through the availability of hybrid instruments that blur the boundaries between military and non-military activity. States can simultaneously employ military signalling, information operations, cyber activities, economic leverage, and proxy networks. The interaction of these instruments generates ambiguity regarding attribution, legality, and proportional response. This ambiguity increases the decision-making burden on the stronger adversary and complicates the management of escalation.

Within this framework, distributed deterrence functions as the operational mechanism through which deterrence of inconvenience is produced. Instead of relying on territorial defence or the threat of overwhelming retaliation, the weaker actor attempts to create a network of cross-domain disruptions that affect logistics, political legitimacy, financial systems, and regional stability. Lessons drawn from asymmetric maritime denial demonstrate how relatively inexpensive and dispersed tools can impose disproportionate operational complications on technologically superior forces. When similar logic is extended across informational, political, and economic domains, the cumulative effect can increase the practical inconvenience of intervention.

The resulting hybrid posture does not aim to defeat the stronger power outright. Rather, it seeks to disperse the adversary's resources, increase uncertainty, and introduce politically sensitive trade-offs that complicate sustained coercive action. In this sense, distributed deterrence represents the operational architecture through which deterrence of inconvenience is implemented under conditions of extreme power asymmetry.

Asymmetric Conflict Revisited: Exploiting Vulnerability

The theoretical foundation of Venezuela's resistance begins with the doctrine of asymmetric conflict. As defined by Ivan Arreguín-Toft (2001), asymmetric conflict occurs when actors with fundamentally different military capabilities and strategic objectives clash, compelling the weak actor to employ indirect strategies.[6] Success for the weak actor hinges on exploiting the structural and psychological vulnerabilities of the strong. These vulnerabilities often include democratic casualty aversion, dependence on uncontested information superiority, and the structural rigidity of conventional military planning.[7] For Venezuela, the primary vulnerability to exploit is the U.S. public and political threshold for casualties and prolonged regional conflict.

The Blurring Lines: Hybrid Warfare as Conceptual Nexus

Hybrid warfare serves as the methodological nexus for contemporary small-state resistance. Frank Hoffman's (2007) definition highlights the emerging simultaneous use of multiple, flexible types of warfare, deliberately blending conventional, irregular, informational, and economic instruments.[8] This strategy allows the aggressor to evade clear attribution and blur the legal and operational boundaries of conflict, maximizing uncertainty for the strong actor. Hybridity allows Venezuela to impose costs across domains simultaneously, which is crucial for maximizing friction against a technologically superior opponent.

Distributed Deterrence and Cost Imposition: Moving Beyond Territorial Defence

The strategic objective of this hybrid methodology aligns with the concept of distributed deterrence, which functions as the operational mechanism through which deterrence of inconvenience is produced. This approach suggests that modern deterrence for weaker states does not rely on territorial parity or conventional military balance. Instead, deterrent effects emerge from the ability to impose distributed, cross-domain costs that complicate the operational and political environment of a stronger adversary. Rather than attempting to defeat the adversary militarily, the weaker state seeks to ensure that any coercive action generates disruptive consequences across multiple domains.

In the Venezuelan context, deterrence of inconvenience operates by creating the expectation that U.S. actions will trigger ripple effects beyond the immediate military domain. These effects may include disruptions to regional energy markets, the activation of information campaigns designed to mobilize domestic and international opposition, and the involvement of regional political actors capable of transforming a limited military operation into a broader diplomatic crisis. The cumulative effect is intended to increase the political and strategic complexity of intervention, thereby raising the perceived costs associated with coercive action.

The dynamics surrounding "Operation Absolute Resolve" (2026) provide a useful illustration of both the relevance and the limitations of this framework. The operation demonstrated the United States' capacity to rapidly conduct a coordinated decapitation strike against Venezuelan leadership using integrated cyber, airpower, and

special operations capabilities.[9] However, the broader regional response highlighted the potential for distributed political and informational effects. The operation immediately triggered intensified diplomatic reactions across parts of Latin America, renewed debates over sovereignty and external intervention, and heightened information campaigns framing the event as evidence of U.S. hegemonic overreach. Although these responses did not prevent the operation itself, they contributed to a broader political environment in which the strategic consequences of intervention extended beyond the immediate tactical success of the strike.[10]

This example illustrates the logic underlying distributed deterrence. Even when a stronger power retains overwhelming military superiority, hybrid strategies can generate secondary disruptions that complicate the political and diplomatic aftermath of intervention. In this sense, deterrence of inconvenience does not aim to prevent action outright. Rather, it seeks to ensure that any intervention produces cascading complications across political, informational, and regional domains, thereby transforming a limited military action into a more complex strategic undertaking.

The Evolving Calculus of Asymmetric Deterrence

The global security environment is undergoing a significant transformation in how power is exercised, challenged, and restrained. Traditional deterrence, rooted in the logic of military parity and territorial defence, is increasingly strained in a strategic environment characterized by rapid technological diffusion and hybrid forms of conflict. The events surrounding "Operation Absolute Resolve" (2026) illustrate this shift. The operation demonstrated the ability of a technologically superior power to combine cyber operations, precision airpower, and special operations forces to neutralize defensive structures and disrupt centralized leadership within a short operational timeframe. This episode revealed the vulnerability of conventionally weak states when confronted with highly integrated military capabilities.[11]

Such developments highlight the growing limitations of classical deterrence models for weaker states. Deterrence by denial becomes difficult when a stronger adversary can rapidly suppress defensive systems and penetrate command structures. Deterrence by punishment is similarly constrained when the weaker state lacks the capacity to impose meaningful retaliation against a superior military power. Under conditions of extreme asymmetry, weaker states must therefore adapt their strategic posture to influence the decision-making calculus of stronger adversaries.

This transformation has been reinforced by the diffusion of relatively low-cost technologies such as drones, cyber capabilities, and unmanned maritime systems. These tools do not eliminate power disparities, but they enable weaker actors to generate disruptions that complicate conventional military superiority. Rather than relying on the ability to defeat an opponent outright, weaker states may attempt to create friction across multiple domains including political, informational, economic, and technological spheres.

Within this environment, weaker actors increasingly pursue what this article conceptualizes as deterrence of inconvenience. This strategy seeks to discourage coercive action by generating persistent operational complications and political costs for the stronger adversary. Instead of preventing intervention outright, deterrence of inconvenience operates by multiplying disruptions that make escalation more complex, time-consuming, and politically costly. Such measures may include irregular maritime activities, proxy mobilization, information operations, and the cultivation of external strategic partnerships.

The Venezuelan case must therefore be understood within this broader evolution of asymmetric deterrence. Although "Operation Absolute Resolve" demonstrated the United States' capacity to rapidly overwhelm conventional defensive structures, it also highlights the strategic incentives for weaker states to adopt hybrid strategies designed to complicate intervention. In this context, deterrence no longer depends solely on military parity or territorial denial. Rather, it increasingly reflects the capacity of weaker actors to generate persistent friction that alters the political and operational calculus of stronger powers.

The Post-Conventional Deterrence Environment: Lessons from Ukraine

The contemporary global strategic landscape has undergone a profound transformation amid the resurgence of great power competition, most visibly manifested in the ongoing Russia–Ukraine conflict. This conflict has illuminated the erosion of traditional conventional deterrence models, where large, high-cost military platforms prove vulnerable to low-cost, distributed disruption technologies.[12] The successful use of unmanned surface vessels (USVs), drones, and improvised weapons by Ukraine to restrict the operations of the superior Russian Black Sea Fleet demonstrates a pivotal shift. Deterrence is increasingly measured not by the capacity to achieve military parity or definitive territorial control, but by the ability to maximize political and operational inconvenience for the strong actor, a strategy centred on cost-imposition.[13]

Coercion, Isolation, and the Quest for Venezuelan Sovereignty

Venezuela presents a critical case study in this evolving environment. The nation is structurally weak, characterized by immense geopolitical resource wealth but severely limited conventional military capacity, operating under comprehensive U.S. coercive measures. These measures include enduring economic sanctions, financial warfare that has acted as a modern siege, restricting Venezuela's oil revenue access and causing widespread over-compliance from international financial institutions, exacerbating the economic crisis.[14] Concurrently, Venezuela faces robust U.S. military posturing in the Caribbean, described as the largest naval deployment in the region since the 1962 Cuban Missile Crisis.[15] The core challenge of Venezuela is identifying how a state lacking fundamental conventional capacity can protect its regime and sovereignty against an overwhelming regional adversary.

Hybrid Asymmetry as a Strategy of Cost Imposition and Temporary Survival

The analysis suggests that Venezuela's strategic posture is not designed to defeat the United States in a conventional military sense or to achieve parity with a vastly superior adversary. Instead, the Venezuelan approach has focused on constructing a multi-domain hybrid resistance architecture intended to complicate and politically burden potential intervention. Through a combination of maritime disruption, informational operations, proxy mobilization, and external partnerships, the strategy attempts to generate friction that raises the operational and political costs of coercive action. In this sense, the Venezuelan posture reflects what this study conceptualizes as deterrence of inconvenience, whereby the objective is not decisive deterrence but the multiplication of complications that make intervention more difficult and politically costly.

The experience of "Operation Absolute Resolve" underscores both the rationale and the limitations of this approach. The operation demonstrated the ability of a technologically superior

power to bypass Venezuela's conventional defensive structures through rapid, intelligence-driven operations. However, the broader strategic logic of hybrid asymmetry remains rooted in the recognition that sustained coercion against the regime relies primarily on long-term economic and political pressure rather than immediate military occupation. For Venezuelan leadership, the United States' economic sanctions regime represents the principal instrument of coercion, forcing the state to divert limited resources toward strategies of political and institutional survival.

Venezuela's Geostrategic Context and Structural Asymmetry

The Coercive Environment: U.S. Power Projection and the Financial Siege

Venezuela operates within a strategic environment defined by profound structural asymmetry vis-à-vis the United States. This asymmetry manifests through two mutually reinforcing forms of coercion: overwhelming kinetic superiority and sustained financial pressure. Together, these elements create a coercive environment that significantly constrains Venezuela's strategic options and shapes its reliance on hybrid resistance strategies.

The kinetic dimension of this asymmetry is reflected in the scale of U.S. military power projection in the Caribbean basin. In the months preceding "Operation Absolute Resolve" (2026), the United States deployed one of the largest regional military buildups in decades, including aircraft carriers, advanced fighter aircraft such as F-35s, strategic bombers, and thousands of personnel operating from regional bases and naval platforms.[16] Such deployments provided the operational infrastructure that enabled the United States to conduct rapid strikes and ultimately execute the operation that captured Venezuelan leader Nicolás Maduro.

Alongside this kinetic imbalance, Venezuela has faced a sustained campaign of economic and financial pressure designed to isolate the country from global markets. Beginning in 2017 and expanding in subsequent years, U.S. sanctions targeted Venezuela's financial sector and the state oil company PDVSA, effectively restricting the government's access to international financial systems and limiting its ability to export crude oil. Because oil exports account for most of Venezuela's export revenue and fiscal income, these sanctions have had severe consequences for the country's economic stability and energy production.[17]

This financial pressure intensified during the lead-up to "Operation Absolute Resolve." The United States implemented maritime interdictions and seizures of tankers transporting Venezuelan crude, forming part of a broader strategy to constrain the regime's primary economic lifeline. Such measures contributed to declining export volumes and further weakened the financial foundations of the Venezuelan state.

Internal Resilience: The Role of Geographic Complexity and Militarized Civil Defence

Venezuela effectively weaponizes its geography and populace for distributed resistance. Its rugged littoral terrain and dense urban zones, particularly the *barrios* of Caracas, are utilized strategically to complicate potential U.S. ground operations. Furthermore, the mobilization of the Bolivarian Militia, with disputed yet massive claimed strength (over 8 million members activated), creates a distributed territorial defence network.[18] This militia, equipped with small arms, RPGs, and domestically refurbished anti-tank systems, is not designed for conventional warfare but to guarantee urban and irregular resistance upon intervention, echoing the asymmetric warfare challenges faced by U.S. forces in Iraq and Afghanistan.[19]

External Enablers: Strategic Partnerships as Defiance Multipliers

The capacity of Venezuela to sustain defiance against the United States is fundamentally dependent on external logistical, financial, and technological assistance that mitigates the effects of sanctions and technological asymmetry. Formal and informal partnerships with Russia, Iran, and China extend the political and material lifespan of the Venezuelan regime by providing economic credit, energy cooperation, military equipment, and diplomatic backing. These relationships function as defiance multipliers, enabling Caracas to maintain a posture of resistance despite severe financial isolation and military disadvantage. Venezuela has repeatedly sought military and technological assistance from these partners, including requests to Russia for strengthened air-defence systems and aircraft maintenance, expanded radar cooperation with China, and drone technology from Iran.[20]

Beyond material assistance, these partnerships provide important diplomatic shielding. Russia and China have publicly supported Venezuela's sovereignty and criticized U.S. military pressure in the Caribbean, reinforcing Caracas's narrative that external intervention constitutes a violation of international norms.[21] Such diplomatic backing extends the regime's political survivability by ensuring that U.S. coercive actions generate international controversy rather than universal consensus.

At the same time, Washington combines overwhelming demonstrations of conventional power, such as large-scale naval deployments and carrier strike groups in the Caribbean, with localized and targeted kinetic actions including interdictions of suspected narcotics vessels or sanctions enforcement operations. While these measures are intended to be precise and legally justified, they generate contradictory signals that the Venezuelan regime can exploit within the information domain.[22] Limited but visible kinetic actions can be reframed domestically as evidence of indiscriminate aggression, allowing the government to portray the United States as targeting Venezuelan sovereignty and civilian infrastructure.

The dynamics surrounding "Operation Absolute Resolve" (2026) illustrate both the importance and the limits of these external enablers. Despite years of military cooperation with Russia and Iran, and economic engagement with China, Venezuela's externally supported defence architecture proved incapable of preventing a rapid, intelligence-driven decapitation operation by the United States. Analysts have noted that equipment sourced from these partners failed to offset the technological and operational advantages demonstrated by U.S. multi-domain operations during the strike.[23] At the same time, the operation triggered immediate diplomatic condemnation and political reactions from several external partners, highlighting how these relationships still function as political amplifiers of Venezuelan resistance even when they cannot provide direct military protection.[24]

Consequently, external partnerships do not fundamentally eliminate the structural asymmetry between Venezuela and the United States. Instead, they serve a more limited but strategically significant role by extending the regime's capacity for defiance, providing material inputs for hybrid resistance strategies, and amplifying the political consequences of U.S. coercive actions. In the context of deterrence of inconvenience, these partnerships therefore act less as sources of decisive military support and more as instruments that expand the diplomatic, informational, and economic ripple effects of confrontation.

Pillar I: Maritime Asymmetry and Littoral Denial

The Goal: Preventing Uncontested Access to the Caribbean Littoral

Venezuela's primary objective in the maritime domain is to prevent uncontested access to its coastal waters and the broader Caribbean littoral. Given the overwhelming naval superiority of the United States, Venezuelan strategy does not seek sea control but rather the creation of a limited anti-access environment designed to complicate naval encirclement, interdiction operations, and potential amphibious landing scenarios. This defensive posture relies on a combination of conventional assets, coastal defence exercises, and hybrid maritime tactics intended to raise the operational risks of operating close to Venezuelan territory.

A key component of this approach is the integration of Russian-supplied Su-30MKV multirole fighter aircraft into Venezuela's littoral defence architecture.[25] The emphasis on coastal denial became particularly visible during the escalation preceding "Operation Absolute Resolve." As the United States deployed carrier strike groups, amphibious vessels, and thousands of personnel to the Caribbean as part of the broader "Operation Southern Spear" buildup, Venezuela responded by conducting large-scale coastal defence drills involving naval and air units. These exercises were explicitly framed by Venezuelan officials as preparations to defend national waters against external intervention and to demonstrate the ability to contest foreign naval activity near Venezuelan territory.[26]

From a strategic perspective, these activities illustrate how Venezuela attempts to operationalize deterrence of inconvenience within the maritime domain. While the Venezuelan Navy and Air Force lack the capacity to challenge U.S. Sea control across the Caribbean basin, localized anti-access capabilities can still generate tactical risks for forces operating within the immediate coastal zone. However, the events surrounding "Operation Absolute Resolve" also highlight the structural limits of this strategy. The United States' ability to concentrate carrier-based aviation, amphibious forces, and precision strike assets in the region ultimately demonstrated that Venezuelan anti-access capabilities can delay or complicate operations only within a narrow coastal belt. Top of Form

Low-Cost Innovation and the Black Sea Analogy

The true asymmetric capacity lies in low-cost innovation, drawing heavily from the Ukrainian experience. Ukraine's success in using USVs, drone swarms, and mines to restrict the superior Russian Black Sea Fleet demonstrates that deterrence is achieved by denying uncontested access, not by controlling the sea.[27] Venezuela utilizes this logic by repurposing civilian and commercial vessels into low-cost, expendable platforms, potentially fitted with improvised explosive devices or used for minelaying, to make naval operations prohibitively risky and costly for the U.S. Navy.[28]

Analysis of Requested Capabilities

Detailed requests for military aid highlight a sophisticated, targeted strategy against U.S. technical superiority. Venezuela sought long-range drones (1,000 km range), passive detection equipment, and GPS scramblers from Iran.[29] The request for passive detection and GPS scramblers is particularly significant; these are direct countermeasures designed to protect Venezuelan coastal assets from precision targeting and surveillance. U.S. conventional superiority relies fundamentally on uncontested Intelligence, Surveillance, and Reconnaissance (ISR). If Venezuela can degrade satellite navigation and radar detection, it forces U.S. forces into closer proximity, slower operations, or reliance on less

reliable sensors. This fundamentally raises operational risk, converting technical vulnerability into a potential guarantee of higher casualty rates, a core exploit of Arreguín-Toft's asymmetric theory.

The distributed nature of these mechanisms is summarized below:

Pillar II: Information and Cognitive Warfare

Framing the Conflict: Positioning U.S. Coercion as Neo-Imperialism

The primary strategic objective of Venezuelan information and cognitive warfare is the control of political narratives at both the domestic and regional levels. Through state media, diplomatic messaging, and coordinated information campaigns, the Venezuelan government seeks to frame U.S. coercive actions as violations of national sovereignty and examples of neo-imperial intervention in Latin America. By portraying the conflict through this lens, the regime attempts to transform a confrontation defined by overwhelming military asymmetry into a broader political and ideological struggle.[30]

This narrative strategy became particularly prominent during the escalation preceding and following "Operation Absolute Resolve" (2026). Venezuelan officials characterized U.S. military deployments in the Caribbean and the subsequent decapitation operation as evidence of aggressive external interference designed to undermine Venezuelan sovereignty. Within the domestic information environment, these events were presented as proof of an external threat requiring national unity and resistance. The regime used this framing to reinforce themes of patriotic defence, mobilize internal political support, and justify the continuation of emergency security measures.[31]

Table 1: Mechanisms of Distributed Cost-Imposition in Venezuelan Hybrid Asymmetry

Hybrid Pillar	Primary Strategic Instrument(s)	Targeted U.S. Cost-Imposition Mechanism
Maritime Denial	Coastal Missiles, Repurposed USVs, Iranian Drones/Scramblers	Operational Risk (A2/AD) and Access Denial
Information Warfare	State Media, Cyber/Influence Operations, Narrative Alignment	Political Legitimacy and Decision-Making Friction
Proxy Networks	ELN/FARC Cooperation, Territorial Militia Mobilization	Increased intervention costs through potential insurgency and regional instability
Strategic Partnerships	Financial Support, Technical Transfers, Logistical Maintenance	Sustained Resistance and Neutralization of Sanctions

The vulnerabilities exposed during "Operation Absolute Resolve" help explain the logic behind these capability requests. The operation demonstrated the effectiveness of U.S. ISR dominance, precision targeting, and integrated multi-domain coordination in rapidly neutralizing Venezuelan defensive structures. In response, Venezuelan efforts to acquire passive detection systems, GPS-jamming technologies, and long-range drones can be interpreted as attempts to degrade the ISR architecture that enabled the operation. Within the framework of deterrence of inconvenience, such measures are intended not to defeat U.S. forces outright but to increase uncertainty, slow operational tempo, and raise the perceived risks associated with future intervention.

Source: Author.

At the regional level, the narrative of neo-imperialism also serves a diplomatic function. By presenting U.S. coercion as an example of hegemonic intervention, Venezuela attempts to activate historical sensitivities in Latin America regarding external interference and sovereignty violations. This messaging is directed toward sympathetic governments, regional organizations, and transnational audiences that may view unilateral intervention with scepticism.[32] Within the framework of deterrence of inconvenience, this narrative strategy seeks to generate political friction for the United States. If Washington escalates its military involvement, it risks reinforcing the Venezuelan government's portrayal of U.S. actions as neo-imperial aggression, potentially generating diplomatic backlash and domestic criticism in the region.

Digital Disruption and Strategic Alignment

While details are often obscured, the threat of cyber operations against regional information systems or U.S. critical infrastructure serves as symbolic, cross-domain deterrence. This low-cost method signals the capacity for distributed disruption, contributing to the overall calculus of risk. Furthermore, influence operations utilize disinformation and diplomatic channels, such as lodging a complaint with the UN Secretary-General, to erode U.S. international legitimacy.[33] The regime actively coordinates its narratives with Russian and Iranian state media, amplifying counter-U.S. messaging globally and extending the cognitive battlefield beyond the immediate Caribbean region, exemplified by Russia's immediate criticism of U.S. strikes.[34]

Following "Operation Absolute Resolve" (2026), for example, Russian officials and state media outlets quickly condemned U.S. actions, framing the operation as an unjustified violation of national sovereignty. This amplification illustrates how aligned narratives can expand the cognitive battlefield and magnify the political visibility of localized military actions.[35]

Weaponizing Domestic Suffering and the Legitimacy Calculation

A sophisticated element of this informational strategy involves redirecting domestic suffering outward. Despite widespread public deprivation, internal repression (such as arresting economists for publishing inflation data), and hyperinflation (estimated at 269.9% in 2025), the regime successfully attributes the economic crisis solely to an "economic war" waged by the U.S..[36] This approach compensates for the regime's failure to achieve "output legitimacy" (the provision of public goods and services) by maximizing "input legitimacy"—the defense of the nation against a perceived existential external threat. The informational strategy thus functions as a mechanism for political survival, diverting public attention from government mismanagement toward external threat perception.[37]

Within the framework of deterrence of inconvenience, this narrative strategy also carries external implications. By emphasizing humanitarian suffering and externalizing blame, the regime increases the reputational costs associated with further coercive measures. Escalation risks reinforcing international perceptions that external pressure is responsible for worsening humanitarian conditions. In this way, domestic economic hardship becomes integrated into the broader informational strategy, functioning both as a mechanism of internal political survival and as a tool for shaping the international legitimacy debate surrounding U.S. intervention.

Pillar III: Proxy and Paramilitary Networks

The Strategic Threat: Guaranteed Urban and Cross-Border Insurgency Post-Intervention

A central component of Venezuela's resistance strategy is the expectation that any external military intervention would rapidly transform into a prolonged and decentralized insurgency. Rather than attempting to defeat a technologically superior adversary through conventional means, the regime's strategy relies on ensuring that intervention cannot produce a quick or decisive victory. The implicit threat is that military action would immediately generate widespread urban resistance, militia mobilization, and cross-border instability.

This logic reflects what can be described as a form of deterrence of inconvenience in which the costs of intervention emerge not from conventional military defeat but from the certainty of prolonged instability. Venezuela possesses several structural conditions that could facilitate such a scenario. The country maintains a large paramilitary and militia network, including pro-government colectivos, irregular armed groups that operate in urban neighbourhoods and support the Bolivarian political movement. These groups could potentially transition from regime support roles to irregular resistance in the event of foreign intervention.

In this sense, the threat of insurgent disorder functions as a component of deterrence of inconvenience. The Venezuelan strategy does not rely on preventing intervention outright. Instead, it seeks to ensure that any attempt at regime change would be followed by prolonged instability, urban resistance, and regional spillover. By signalling that intervention would create a complex and politically costly post-conflict environment, the regime attempts to influence the strategic calculus of external actors considering coercive action.

Regime-Proxy Symbiosis and Control over Illicit Economies

The regime maintains a "selective" cooperation with U.S.-designated terrorist groups of Colombian origin, notably the National Liberation Army (ELN), FARC-EP, and Segunda Marquetalia. The regime provides safe-haven, enabling these groups to operate across large portions of Venezuelan territory and profit from illicit activities, including drug and human trafficking, establishing financial ties with elements of the Venezuelan state. The ELN has formed symbiotic relationships with Venezuelan military and security officials to facilitate and protect trafficking routes.[38]

This relationship is not passive. Venezuelan security, military, and national guard forces have reportedly directly coordinated operations against one FARC dissident faction (FARC-EP) alongside the rival ELN in border areas.[39] This explicit cooperation transforms a state weakness (lack of border control) into a strategic asset (a complex, lethal proxy buffer zone).

The Tactical Role of the Bolivarian National Militia

The loyalist, non-state armed groups, primarily the massive Bolivarian Militia serve as the foundation for territorial defence, allowing the conventional military to prioritize high-end deterrent assets (like the Su-30s). The militia's training focuses on maximizing the home-field advantage and employing distributed small-unit resistance in urban terrain to elevate the expected casualty rates for U.S. forces.[40] This devolution of security control is a clear application of the hybrid model, ensuring resistance is decentralized and highly attritional.
Bottom of Form

Pillar IV: Strategic Partnerships and Collective Asymmetry

Venezuela's ability to sustain its hybrid defence posture rests on its informal coalition of partners, collectively providing "collective asymmetry" that neutralizes the sanctions regime and technical gaps.

Russian Logistics and Air Defence Support

Russia is critical for maintaining Venezuela's conventional deterrent capacity. Venezuelan President Nicolás Maduro described Russian-made Sukhoi Su-30MK2 fighters as the "most important deterrent" against the threat of war. Maduro has requested specific assistance from Russia, including the restoration of several Sukhoi aircraft, overhaul of engines and radars, the acquisition of fourteen missile units, and a "medium-term financing plan of three years" through Rostec.[41] Russia further provides necessary advisory, intelligence, and technical support, ensuring that Venezuela's limited high-end assets remain credible and operational.[42]

Iranian Technical Transfers

Iran serves as the source for crucial, combat-proven hybrid technology transfers, enabling tactical asymmetry. Requested Iranian assets include long-range drones (1,000 km range), GPS scramblers, and passive detection equipment. This relationship allows Venezuela to rapidly and cheaply acquire force multipliers specifically tailored to disrupt U.S. surveillance and targeting capabilities, effectively countering U.S. technical superiority by distributing anti-ISR capacity.

Chinese Cyber and Radar Technology

China contributes to the resilience of Venezuela's command, control, and early warning systems. Maduro sought "expanded military cooperation" and requested that China expedite production of radar detection systems. China provides critical digital infrastructure support, hardening the state against U.S. digital coercion and surveillance and enhancing situational awareness.[43]

The Mechanics of "Collective Asymmetry" and the Paradox of Defiant Dependence

Venezuela strategically attempts to weaponize the shared ideology among its patrons, framing potential U.S. military action against Venezuela as "action against China." This tactic raises the political cost of intervention by introducing strategic uncertainty, transforming a local conflict into an indirect confrontation between great powers—a significant factor in achieving distributed deterrence.

However, this reliance creates the paradox of defiant dependence. While Venezuela achieves temporary sovereignty through defiance of the U.S., this defiance is structurally predicated on deep, long-term technical and financial dependence on the parallel coalition. By requiring a three-year financing plan via Rostec and relying on Iranian technology transfers, Venezuela trades dependence on the Western system for dependence on an anti-Western coalition.[44] This limits genuine state autonomy, ensuring regime survival but not self-sufficiency.

The limitations of this model became evident during "Operation Absolute Resolve" (2026). Despite years of external military cooperation, Venezuelan air defence and surveillance systems failed to prevent the rapid U.S. strike that neutralized key military infrastructure and enabled the capture of Nicolás Maduro. The episode revealed that external partnerships can sustain resistance and prolong defiance but remain insufficient to offset the technological and operational advantages of a major military power.

The Limits and Costs of Hybrid Deterrence

Despite its ability to generate a form of deterrence of inconvenience, hybrid asymmetry remains a

Table 2: Strategic Function of External Enablers in Venezuela's Hybrid Deterrence

Partner State	Requested Assets/ Support	Immediate Strategic Function	Conceptual Contribution to Hybrid Deterrence
Russia	Sukhoi Restoration, Missiles, Rostec Financing	Conventional Deterrence/ Air Defence Credibility	Sustainment of High-End Deterrent Assets and Logistical Endurance
Iran	1000km Drones, GPS Scramblers, Passive Detection	Tactical Asymmetry, Anti-ISR, and Precision Strike	Democratization of Coercive Capacity (Low-Cost Technology Transfer)
China	Expedited Radar Detection Systems, Expanded Cooperation	Situational Awareness, Early Warning, and Cyber Resilience	Infrastructure Hardening and Strategic Warning Time

Source: Author.

fragile and ultimately unsustainable long-term strategy. The Venezuelan case illustrates how hybrid deterrence may complicate external intervention while simultaneously imposing severe internal costs on the state itself.

Organizational and Operational Fragility

Hybrid strategies require a high degree of organizational coordination across multiple domains, including conventional forces, intelligence services, proxy actors, and external logistical networks. Such arrangements demand strong institutional capacity and reliable command structures capable of synchronizing operations across these diverse actors. Fragile states often lack the administrative depth, professional military capacity, and interagency coordination necessary to sustain complex hybrid operations over extended periods.

The vulnerabilities of such structures became evident during "Operation Absolute Resolve" (2026). The U.S. operation relied on tightly integrated intelligence, cyber operations, and special forces coordination involving more than 150 aircraft launched from multiple locations across the Western Hemisphere. The rapid suppression of Venezuelan air defences and the capture of President Nicolás Maduro within a few hours demonstrated how highly integrated military operations can exploit organizational weaknesses within hybrid defence systems.[45]

Intelligence and Cyber Superiority

Another structural limitation lies in the persistent intelligence advantage maintained by the United States. While Venezuela has attempted to acquire anti-ISR capabilities such as GPS jammers, passive detection systems, and long-range drones, the United States retains overwhelming superiority in global surveillance networks, cyber capabilities, and signals intelligence.

The success of "Operation Absolute Resolve" was heavily dependent on detailed intelligence about Maduro's movements and security arrangements, gathered over months of surveillance and intelligence coordination.[46] This level of intelligence penetration allowed U.S. forces to conduct a targeted decapitation operation with a high degree of precision. The episode illustrates how hybrid deterrence strategies that rely on distributed disruption remain vulnerable when confronted with adversaries capable of penetrating command structures and neutralizing key nodes of coordination.

Economic Exhaustion and Resource Misallocation

The most severe limitation of hybrid deterrence arises from economic exhaustion. While hybrid warfare techniques can be relatively inexpensive compared with conventional force modernization, they do not address the structural economic pressures imposed by long-term sanctions and financial isolation. Venezuela's economy has suffered a dramatic contraction due to sanctions targeting its oil sector, historically the country's primary source of state revenue.

In response, the Venezuelan state has increasingly diverted resources toward maintaining security structures, patronage networks, and hybrid defence mechanisms. This dynamic produces a form of resource misallocation in which scarce economic capacity is directed toward sustaining political survival rather than rebuilding state institutions or generating long-term economic growth. Hybrid deterrence therefore functions as a resource-reallocating strategy rather than a resource-generating one, prolonging regime survival without resolving the underlying economic crisis.

The Legitimacy Paradox: Sovereignty Defended Through Instability

The reliance on hybrid strategies also produces a profound legitimacy paradox. On the one hand, the regime attempts to defend its formal sovereignty and resist external coercion. On the other hand, the mechanisms used to sustain this resistance often undermine the internal legitimacy and institutional stability of the state.

Cooperation with irregular armed actors and proxy groups weakens the rule of law and contributes to the fragmentation of state authority. As governance increasingly relies on coercive mechanisms and informal armed networks, the state's capacity to provide public goods and maintain institutional credibility erodes. In political terms, the regime struggles to maintain output legitimacy, defined as the ability to deliver economic stability and public services, while also facing challenges to input legitimacy, or democratic representation and consent.

Policy Implications and Options for U.S. Coercive Strategies

The experience of "Operation Absolute Resolve" (2026) demonstrates both the effectiveness and the limitations of conventional U.S. coercive power. The operation involved a coordinated multi-domain assault to capture Venezuelan president Nicolás Maduro in Caracas within a few hours. While the mission successfully neutralized Venezuelan leadership and exposed the weakness of its conventional defences, the broader strategic environment surrounding the intervention revealed the resilience of Venezuela's hybrid resistance architecture and the persistence of political backlash at both regional and international levels. Although the operation succeeded tactically, it did not eliminate the structural foundations of Venezuela's hybrid defence architecture.

For the United States, this outcome suggests that conventional kinetic superiority alone is insufficient to resolve conflicts characterized by hybrid resistance strategies. Highly visible military actions may unintentionally reinforce the Venezuelan government's narrative of external aggression, thereby strengthening the regime's justification for acquiring external military support and expanding hybrid defence mechanisms. An effective U.S. counter-strategy therefore requires a more comprehensive approach that addresses the structural foundations of Venezuela's hybrid deterrence.

1. Decoupling the Regime from Hybrid Enablers

The most critical objective should be the disruption of the external networks that sustain Venezuela's hybrid defence posture. Russia, Iran, and China collectively provide logistical maintenance, surveillance technologies, and hybrid military capabilities that compensate for Venezuela's domestic weaknesses.

2. Strategic Focus on Proxy Networks

A second priority involves addressing the regime's reliance on irregular armed actors and illicit economic networks. Venezuelan hybrid strategy partially depends on the ability to mobilize non-state groups and exploit illicit economies that generate both financial resources and regional instability. Counter-coercion strategies should therefore focus on dismantling these support structures by targeting trafficking networks, restricting cross-border safe havens, and strengthening regional law-enforcement cooperation.

3. Reframing the Coercion Narrative

A third policy priority involves the information domain. Venezuelan information strategy attempts to portray U.S. coercive actions as neo-imperial aggression, thereby strengthening the regime's claims to political legitimacy as the defender of national sovereignty. To counter this narrative, U.S. strategy must visibly address the humanitarian and economic needs of the Venezuelan population while distinguishing between pressure directed at the regime and support directed at Venezuelan society. Targeted humanitarian assistance, economic stabilization measures, and diplomatic engagement with regional organizations could reduce the effectiveness of the regime's narrative framing.

Conclusion: Operation Absolute Resolve and the Resilience of Hybrid Resistance

This study has examined how a conventionally weak state attempts to resist coercion from a materially superior adversary through hybrid asymmetry. The Venezuelan case demonstrates that modern resistance strategies increasingly rely not on territorial defence or conventional parity, but on the deliberate generation of distributed friction across multiple domains. Through maritime denial, information warfare, proxy networks, and strategic partnerships with external powers, Caracas constructed a hybrid defence architecture designed to impose operational, political, and reputational costs on potential intervention. In this sense, Venezuela's strategy reflects what this study conceptualizes as deterrence of inconvenience, a form of deterrence in which weaker actors seek to complicate coercive action rather than prevent it outright.

Yet the broader political outcome reveals the limits of coercive intervention against hybridized regimes. Despite the capture of Maduro, the Venezuelan state apparatus did not collapse. Vice president Delcy Rodríguez assumed the presidency, and the governing structures of the Bolivarian regime remained intact. The continuation of the regime illustrates a central feature of hybrid warfare: leadership decapitation does not necessarily dismantle the distributed networks of political control, militia mobilization, information campaigns, and external partnerships that sustain regime survival.

In this sense, "Operation Absolute Resolve" demonstrates both the strength and the limitation of hybrid deterrence. Venezuela's hybrid defences were unable to prevent decisive U.S. military action, revealing the structural vulnerability of weak states confronting integrated multi-domain operations. At the same time, the regime's capacity to adapt and continue governing after the removal of its leader

highlights the resilience of hybrid political systems built for survival under sustained pressure.

This dynamic reveals a broader transformation in the logic of resistance in the hybrid age. When denial and punishment are unattainable, weaker states increasingly rely on distributed disruption and strategic ambiguity to shape the costs of coercion. Such strategies do not eliminate power asymmetry, but they can ensure that intervention produces uncertain and politically complex outcomes.

For policymakers, the Venezuelan case underscores the difficulty of using coercive pressure to engineer regime transformation. Economic isolation, military signalling, and targeted strikes may succeed in weakening leadership structures, but they can also reinforce the adaptive survival mechanisms of hybrid regimes. The result is a strategic paradox: coercive success at the tactical level may coexist with political failure at the systemic level.

Ultimately, the Venezuelan experience illustrates the deeper paradox of modern resistance. Hybrid deterrence does not guarantee security, nor can it prevent decisive military action by stronger powers. However, it can enable fragile regimes to survive even severe external shocks. In this environment, sovereignty is preserved not through conventional military strength but through the ability to adapt, distribute disruption, and sustain political control in the face of external intervention. Hybrid asymmetry therefore represents both a symptom of structural weakness and a strategy of endurance in an international system where the weak cannot defeat the strong, but they can refuse to collapse.

Endnotes

[1] Paramjit Singh, "Why Venezuela? Oil, Power, and Ideology," *Critical Sociology*, OnlineFirst, 2026, https://doi.org/10.1177/08969205261422623.
[2] BBC News, "Spies, Drones and Blowtorches: How the US Captured Maduro," January 4, 2026, https://www.bbc.com/news/articles/cdred61epg4o.
[3] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966).
[4] Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004).
[5] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961).
[6] Ivan Arreguín-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security*, Summer 2001, published by the Belfer Center for Science and International Affairs, https://www.belfercenter.org/publication/how-weak-win-wars-theory-asymmetric-conflict-0.
[7] Daniel Ford, review of How the Weak Win Wars: A Theory of Asymmetric Conflict by Ivan ArreguínToft, *The Warbird's Forum*, July 2019, https://www.warbirdforum.com/weakwin.htm.
[8] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).; Murat Caliskan, "Hybrid Warfare Through the Lens of Strategic Theory," *Defense & Security Analysis* 35, no. 1 (2019): 40-58, https://doi.org/10.1080/14751798.2019.1565364.
[9] BBC News, "How the US Captured Maduro."
[10] Kristian Alexander, "Venezuela, 'Absolute Resolve,' and the Return of Coercive U.S. Statecraft in the Western Hemisphere," Rabdan Security and Defense Institute (RSDI), January 16, 2026, https://rsdi.ae/en/publications/venezuela-absolute-resolve-and-the-return-of-coercive-us-statecraft-in-the-western-hemisphere.
[11] Manoj Joshi, "US Operation in Venezuela: Modern Conflict Lessons," *Observer Research Foundation*, January 9, 2026, https://www.orfonline.org/expert-speak/us-operation-in-venezuela-modern-conflict-lessons.
[12] Ayman Eldessouki and Rahaf Al Khazraji, "Asymmetric Warfare and Prospects of the Russia-Ukraine War," TRENDS Research & Advisory, May 6 2024, https://trendsresearch.org/insight/asymmetric-warfare-and-prospects-of-the-russia-ukraine-war/.
[13] Mark Temnycky, "Ukraine Has Innovated Naval Warfare," *Center for Maritime Strategy*, July 31, 2025, https://centerformaritimestrategy.org/publications/ukraine-has-innovated-naval-warfare/.
[14] The Impacts of United States Embargo on Venezuela," *Puspitur*, June 5 2025, https://puspitur.com/2025/06/05/the-impacts-of-united-states-embargo-on-venezuela/.
[15] Jeffrey Fields, "Trump's Anti-Venezuela Actions Lack Strategy, Justifiable Targets and Legal Authorization," USC Dornsife College of Letters, Arts & Sciences, October 29, 2025, https://dornsife.usc.edu/news/stories/trumps-anti-venezuela-actions-lack-strategy-justifiable-targets-and-legal-authorization/.
[16] Steven Nelson, "Trump Says Maduro's Days Leading Venezuela Are Numbered — as US Amasses Largest Caribbean Military Presence in 35 Years," *New York Post*, November 3, 2025, https://nypost.com/2025/11/03/us-news/trump-says-maduros-days-leading-venezuela-are-numbered-as-us-amasses-largest-caribbean-military-presence-in-35-years/.
[17] The Impacts of United States Embargo," Puspitur.; Joseph Federici, Nicole Morgret, Benton Gordon, and Graham Ayres, "China–Venezuela Fact Sheet: A Short Primer on the Relationship," U.S.-China Economic and Security Review Commission, January 13, 2026, https://www.uscc.gov/research/china-venezuela-fact-sheet-short-primer-relationship.
[18] CNN, "Venezuela Announces 'Massive Mobilization' of Military as US Buildup Intensifies," November 11, 2025, https://edition.cnn.com/2025/11/11/americas/venezuela-military-mobilization-us-buildup-intl-latam.
[19] Allen Frazier, "What U.S. Forces Face as Venezuela Puts Russian-Armed Military on Wartime Alert," *Military.com*, October 20 2025, https://www.military.com/daily-news/investigations-and-features/2025/10/20/what-us-forces-face-venezuela-puts-russian-armed-military-wartime-alert.html.
[20] "Venezuela Asks Russia, China, Iran for Help in Connection with US Pressure — Newspaper," *TASS*, October 31, 2025, https://tass.com/world/2038269.; "Venezuela Turns to Iran, Russia, China for Military Aid amid US Buildup," Iran International, November 1, 2025, https://www.iranintl.com/en/202511019541.
[21] Alperen Aktaş, "Russia Backs Venezuela's 'Sovereignty,' Urges Dialogue after US Military Operation," *Anadolu Agency*, January 6, 2026, https://www.aa.com.tr/en/world/russia-backs-venezuela-s-sovereignty-urges-dialogue-after-us-military-operation/3791628.; Cristina Guevara, "China's Support for the Maduro Regime: Enduring or Fleeting?" *Atlantic Council – New Atlanticist*, January 13, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/chinas-support-for-the-maduro-regime-enduring-or-fleeting/.

[22] Center for Economic and Policy Research (CEPR), "US Escalation in the Caribbean and Latin America (Americas Live Updates)," accessed March 9, 2026, https://cepr.net/publications/americas-live-updates/.
[23] Seth J. Frantzman, "When Caracas Cracked: How the US Broke Through Venezuela's Iranian, Russian, and Chinese Defenses," *The Jerusalem Post*, December 2025, https://www.jpost.com/defense-and-tech/article-882802.
[24] Akriti Anand, "How China, UK, Russia, India, Pakistan, Iran, France Reacted to US Bombing of Venezuela: 'We Shed No Tears…'," *Mint (LiveMint)*, January 4, 2026, https://www.livemint.com/news/world/venezuela-us-bombing-how-china-uk-russia-india-pakistan-iran-france-react-we-shed-no-tears-president-nicolas-maduro-11767402429612.html.
[25] "Venezuela's Anti-Ship Missile Capabilities: Assessing Coastal Defence Architectures in the Caribbean Theater, 2025," *Debuglies*, October 23, 2025, https://debuglies.com/2025/10/23/venezuelas-anti-ship-missile-capabilities-assessing-coastal-defense-architectures-in-the-caribbean-theater-2025/.
[26] "Venezuela Launches Coastal Defence Drills Amid U.S. Military Build-Up," *Iranian Students' News Agency* (ISNA), 26 October 2025, https://en.isna.ir/news/1404080402037/Venezuela-launches-coastal-defense-drills-amid-US-military-build-up.
[27] Raveendran, Jithin. „Sea Denial: The Ukrainian Case Study and the Future of Naval Warfare." *Journal of Strategic Security* 18, no. 4 (2025) 96-111. DOI: https://doi.org/10.5038/1944-0472.18.4.2564.
[28] Evan Cooper and Alessandro Perri, "The Strategic Costs of US Strikes Against Venezuela," *Stimson Center*, October 10, 2025, https://www.stimson.org/2025/the-strategic-costs-of-us-strikes-against-venezuela/.
[29] Maria Tril, "Washington Post: Venezuela Seeks Russian Weapons, Chinese Radars, Iranian Drones amid Reported U.S. Military Pressure," *Euromaidan Press*, October 31, 2025, https://euromaidanpress.com/2025/10/31/washington-post-venezuela-seeks-russian-weapons-chinese-radars-iranian-drones-amid-reported-us-military-pressure/.
[30] Azizi Othman, "Sovereignty Under Siege: The 2026 Venezuelan Intervention and the Crisis of the Westphalian Order," January 2026, https://doi.org/10.13140/RG.2.2.14210.13761.
[31] Ibid.
[32] Huberman, Bruno, and Rodrigo Augusto Duarte Amaral. 2025. "Hegemony and Resistance: US Imperial Strategies in Latin America and the Middle East After the Cold War." *Middle East Critique* 34 (4): 581–606. doi:10.1080/19436149.2025.2578046.
[33] "US-Venezuela Strains Spike amid Escalating Naval Buildup," *Daily Sabah*, August 29, 2025, https://www.dailysabah.com/world/americas/us-venezuela-strains-spike-amid-escalating-naval-buildup.
[34] "Defence Experts Warn U.S. Warship Deployment Near Venezuela Could Face Threat from Russian-Made Missiles," *Latin Times*, October 22, 2025, https://www.latintimes.com/defense-experts-warn-us-warship-deployment-near-venezuela-could-face-threat-russian-made-missiles-590808.
[35] Anshu Kumar, "Contextualising Russian Responses to US Military Action in Venezuela," *Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA)*, February 10, 2026, https://idsa.in/publisher/comments/contextualising-russian-responses-to-us-military-action-in-venezuela.
[36] "Maduro Braces for a U.S. Attack; Venezuelans Are More Worried About Dinner," *The Washington Post*, November 1, 2025, https://www.washingtonpost.com/world/2025/11/01/maduro-venezuela-attack-economy/.

[37] OECD, *The State's Legitimacy in Fragile Situations: Unpacking Complexity* (Paris: International Network on Conflict and Fragility, OECD, 2010), https://gsdrc.org/document-library/the-states-legitimacy-in-fragile-situations-unpacking-complexity/.
[38] U.S. Department of State, *Country Reports on Terrorism 2022: Venezuela*, https://www.state.gov/reports/country-reports-on-terrorism-2022/venezuela/.
[39] U.S. Department of State, *Country Reports on Terrorism 2022: Venezuela*.
[40] Allen Frazier, "What U.S. Forces Face as Venezuela Puts Russian-Armed Military on Wartime Alert," *Military.com*, October 20, 2025, https://www.military.com/daily-news/investigations-and-features/2025/10/20/what-us-forces-face-venezuela-puts-russian-armed-military-wartime-alert.html. Military.com.
[41] Tril, "Washington Post: Venezuela Seeks Russian Weapons."
[42] Andrew S. Radin and Theodore R. Johnson, "Russia's Intervention in Venezuela: What's at Stake?" (Policy Brief, Atlantic Council, September 2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/09/Russia-Venezuela-Policy-Brief.pdf.
[43] Fatma Zehra Solmaz, "Maduro Turns to Moscow, Beijing, Tehran as US Presence Builds in Caribbean," *Anadolu Agency*, November 1, 2025, https://www.aa.com.tr/en/americas/maduro-turns-to-moscow-beijing-tehran-as-us-presence-builds-in-caribbean/3732330.
[44] Tril, "Washington Post: Venezuela Seeks Russian Weapons."
[45] BBC News, "How the US Captured Maduro."
[46] Ibid.

The Contested Kinmen Model

Infrastructure as Irregular Warfare in the Taiwan Strait

By Ian Murphy

Introduction: Learning from Kinmen's Modern History and the Kinmen Model

Kinmen County, Taiwan, stands as an anomaly in East Asia—it is an archipelago administered by Taipei but visually and geographically tethered to the coastline of the People's Republic of China (PRC). For over seven decades, these islands have served as the physical frontline of the unfinished Chinese Civil War, functioning first as a kinetic battleground and later as a laboratory for cross-strait engagement. Yet, to view Kinmen as a relic of the Cold War is to miss its contemporary strategic significance. The region has now become the primary theater for the PRC's "Kinmen Model" (*Jinmen Moshi,* 金門模式), a strategy that weaponizes proximity and developmental needs to erode sovereignty from within. Understanding this current campaign of irregular warfare requires first tracing the island's unique trajectory, which reveals how historical legacies of isolation have created the very structural vulnerabilities that Beijing now exploits.

Kinmen's modern existence is defined by a dynamic, four-phase relationship with mainland China, having transitioned from a Cold War military frontline to a hub of economic exchange. However, this history did not cease evolving with the economic détente of the early 21st century. The publication of "Securitizing Kinmen" established that Taiwan's traditional four-period historical framing is insufficient for explaining contemporary cross-strait dynamics, necessitating the recognition of a distinct fifth period—the Era of the Contested Kinmen Model. This shift marks the culmination of the prior phases and serves as the immediate political and conceptual justification for China's infrastructure mega-projects.

Kinmen's historical periods underscore a progressive strategic demilitarization, which China now exploits:

The transition into the Fifth Period is fundamentally defined by the rise of the Kinmen Model, which the People's Republic of China aggressively promotes through its state media.[1] While presented as a benign

Ian Murphy is a PhD student in International Studies at Old Dominion University, specializing in China's geoeconomic strategy and gray-zone warfare. He holds an MBA from National Taiwan Normal University as well as an MA in National Security Studies. In addition to his doctoral research and role as an Adjunct Instructor at ODU, he serves as a China Subject Matter Expert for SecuriFense Inc. in Norfolk, Virginia.

Figure A: Kinmen's Historical Periods

Historical Period	Defining Characteristic	Strategic Implication
First (1949-1958)	Intense Military Confrontation	Symbol of existential cross-strait conflict.
Second (1959-1979)	Defensive Military Fortification	Sustained high military readiness; pervasive influence on civil life.
Third (1980-2000)	Economic Détente	Gradual easing of the "three non-links"; beginning of reassessment.
Fourth (2001-2014)	Border Infiltration; Mini-Three Links	Kinmen was used by Taiwan as an economic testing ground; conduit for trade and tourism with mainland China. The Mini Three Links (2000) established limited postal, transportation, and trade links connecting Kinmen and Matsu with coastal Fujian. The full Big Three Links across the Taiwan Strait were subsequently established in 2008.
Fifth (2014-Present)	The Contested Kinmen Model	Securitization of Taiwan's control by PRC; deployment of gray zone tactics, including the assertion of PRC sovereignty and jurisdiction over Kinmen, emphasis on protecting the interests and safety of Kinmen's fishermen, the gradual expansion and normalization of maritime control, the integration of civilian and security dimensions, and infrastructure coercion. Xi Jinping introduced the Four New Links.

Source: Author.

blueprint for "peaceful cross-strait relations centered on economic and cultural integration," this narrative is, in fact, a deliberate securitization strategy aimed at redefining Kinmen's status from a non-political fact to a political vulnerability.

The PRC's mega-infrastructure projects are the physical manifestation of this new historical era, designed to institutionalize non-kinetic control and create a *fait accompli* of political incorporation. These projects function as instruments of irregular warfare through two primary objectives: structural dependency and cognitive influence.

China's efforts, including the recently operational Jinjiang-Kinmen water pipeline and proposed links for electricity, gas, and a bridge, are aimed at creating an infrastructural chokepoint. The infrastructure links Kinmen's essential life domains (water, energy, and transportation) directly to mainland China, forcing the island into a state of structural coercibility. This is a deliberate inversion of the traditional dependency paradigm (which relies on exploitation), substituting positive resource flow (freshwater) to generate political leverage.

Beyond material control, the infrastructure projects are powerful tools of cognitive warfare. By resolving chronic developmental bottlenecks like water scarcity, the PRC gains significant political goodwill and influences local decision-making structures. This strategic injection of resources manipulates the local populace and leadership to prioritize the immediate, tangible benefits of integration (stable water supply, economic expansion) over the abstract, long-term risk of strategic autonomy. The construction of physical links is

seamlessly integrated with state media narratives that promote distrust of the Taiwanese central government and amplify the promise of prosperity, thereby eroding Taipei's effective control and advancing the conceptual framework of the Kinmen Model as the new, integrated reality. This long-term, non-kinetic strategy of infrastructure coercion aims to set a profound psychological and political precedent for eventual reunification.

The Conflict Over Kinmen Connectivity: Taiwanese and Mainland Chinese Perspectives

Following decades of sustained military readiness and pervasive influence on civil life, the gradual easing of the Cold War environment culminated in the establishment of the Mini Three Links (小三通). Launched in the year 2000, this program of limited postal, transportation, and trade links connected Kinmen and Matsu with coastal areas in Fujian Province.[2] The primary objective of the Mini Three Links, from Taiwan's perspective, was to provide a legal basis for managing petty smuggling occurring between Kinmen, Matsu, and Fujian Province. The program also served as an experiment intended to inform the subsequent launch of the full Big Three Links (direct postal connections, commerce, and transportation) across the entire Taiwan Strait, extending from the outlying islands to cover the majority of Taiwan's territory, later established in 2008.[3] The policy initially prioritized national security while regulating the cross-border flow of personnel and goods to provide convenience for residents and businesses.

Since its inception, the Three Mini Links played a significant and positive role in facilitating people-to-people exchanges. Between 2001 to 2023, the four Mini Three Links routes between Fujian and Taiwan have completed 225,413 voyages, transporting more than 22 million passengers.[4] Specifically, the Xiamen-Kinmen route has transported over 19.81 million passengers, the Quanzhou-Kinmen route 1.39 million, the Matsu-Mawei route 660,000, and the Matsu-Huangqi route 190,000.[5] The launch of the ferry service further helped transform the Kinmen islands into a magnet for Chinese tourists and boosted the local economy. However, the effectiveness of the Mini Three Links was severely disrupted during the COVID-19 pandemic, leading to the temporary suspension of passenger services by the Tsai Ing-wen Administration in 2020 to curb the spread of COVID into Taiwan.[6]

The era of limited, negotiated exchanges defined by the Mini Three Links was dramatically challenged by China's aggressive push for deeper integration under Xi Jinping, ushering in the Era of the Contested Kinmen Model.[7] In a January 2, 2019, speech commemorating the 40th anniversary of the "Message to Compatriots in Taiwan," CCP General Secretary Xi Jinping formally announced the "New Four Links" (新四通) program.[8] Xi proposed that the two sides of the Taiwan Strait should promote connectivity in areas including infrastructure building as well as energy and resource development. The program specifically advocates four forms of connectivity between Fujian coastal areas and Kinmen and Matsu, including water (通水), electricity (通電), natural oil and gas (通油/氣), and bridges (通橋). This push for deeper integration is a continuation of Xi's personal interest in cross-strait connectivity, dating back to 1998 when he publicly discussed the importance of a cross-strait tunnel while serving as a middling deputy secretary of the CCP Fujian Provincial Committee.[9]

The purpose of the New Four Links is explicitly tied to Beijing's political objective of reunification, designed to institutionalize non-kinetic control. The ultimate aim is the creation of a "Xiamen-Kinmen Living Circle" (廈金同城生活圈).[10] This concept is intended to bind people from the paired regions together and blur the line between Kinmen and

Xiamen. The systematic normalization of essential resource ties, facilitated by infrastructure, is a mechanism of political normalization intended to achieve a victory without fighting at the local level. This non-kinetic strategy aims to set a psychological and political precedent for eventual complete reunification. This is a shift from the negotiated Mini Three Links to unilateral infrastructure projects aimed at creating structural dependency and coercibility through the act of weaponized interdependence.

Taiwan's Mainland Affairs Council (MAC) has strongly condemned this unilateral shift, characterizing the CCP's goal as incorporating Kinmen into Fujian Province.[11] The MAC views the proposed Kinmen-Xiamen Bridge not as a policy continuation of the Mini Three Links but as a "unilateral proposal of the Chinese Communist Party driven by its united front thinking. They have repeatedly labeled the bridge as a "Trojan horse carrying tremendous national security risks".[12] While the full framework of the Xiamen-Kinmen Living Circle establishes the broader coercive environment, this analysis focuses specifically on the projects designed to create structural and cognitive vulnerabilities: the operational Jinjiang-Kinmen water pipeline, the proposed Kinmen-Xiamen Bridge, and the Xiamen Xiang'an Airport.

Literature Review: Infrastructure as an Instrument of Irregular Warfare

The utilization of civilian infrastructure for strategic, non-military objectives–a hallmark of modern irregular warfare demands a conceptual framework that transcends the boundaries of traditional security and economic theory. In this context, irregular warfare encompasses assertive, non-kinetic actions designed to achieve strategic effects while remaining below the threshold of conventional military conflict. Analyzing the Contested Kinmen Model through this lens requires an understanding of the PRC's unique development path, defined by a version of the Beijing Consensus that subordinates market logic to the political survival of the CCP. By examining the institutional machinery of China Inc. and the resulting security imperative, this literature review progressively reveals the systematic mechanisms that allow seemingly benign civilian infrastructure to function as a coercive strategic weapon.

The Strategic Logic of the Fait Accompli

While the "Contested Kinmen Model" utilizes economic and physical networks, its overarching strategic objective is the creation of a *fait accompli*. In international relations theory, a *fait accompli* is defined by Dan Altman as a unilateral move to deny an opponent the choice of whether to concede. Unlike coercive diplomacy, which relies on threats to influence an adversary's future behavior, the *fait accompli* seeks to "wrest territory" by presenting the opponent with a completed reality such as a new status quo that is prohibitively costly or risky to reverse.[13] Within this framework, the PRC's "New Four Links" are not a series of bilateral negotiations, but a unilateral attempt to "wrest" Kinmen's functional sovereignty by establishing a physical and logistical reality that Taipei cannot undo without triggering a disproportionate military escalation.

The timing and sequencing of these projects follow the logic of "salami tactics," a progression of limited *faits accomplis* that individually appear manageable but are cumulatively transformative. Richard Maass posits that these tactics are most effective when executed "in the shadow of major war," where the target is deterred from escalating over a single, relatively minor revision to the status quo.[14] The evolution from the Jinjiang-Kinmen Water Pipeline to the proposed Kinmen-Xiamen Bridge and the massive Xiang'an International Airport illustrates this incrementalism. By ensuring that each individual slice–such as a singular pipeline

or the construction of a bridge trestle–remains below the threshold of major conflict, the PRC successfully avoids a decisive confrontation while steadily building the infrastructure necessary for political incorporation.

Finally, the Kinmen projects represent what Dr. Joshua Hastey identifies as China's specific preference for physical revisions to the status quo to institutionalize control. Hastey's work on China's maritime *faits accomplis*, through the creation of artificial islands, demonstrates how environmental engineering and fixed infrastructure serve as irreversible markers of authority.[15] This provides the conceptual bridge to the Xiang'an Airport project, where massive land reclamation has already halved the distance between the mainland and Kinmen. By physically altering the geography of the Taiwan Strait, the PRC creates a "*fait accompli*" that is not merely diplomatic but material, using infrastructure as a non-kinetic tool to move Kinmen's survival and governance into the mainland's orbit.

The Institutional Machinery of the Security Imperative

This body of scholarship establishes theoretical and operational legitimacy for analyzing seemingly commercial activities as core instruments of national power. At the foundational level, Joshua Cooper Ramo defines the Beijing Consensus as a "new physics of development and power" that explicitly validates the strategic use of non-military resources.[16] By prioritizing asymmetric power projection, the PRC deliberately leverages economic strength and technological influence over conventional military force to defend its interests. For Kinmen, this lens immediately reframes infrastructure as a tool of asymmetric engagement rather than mere civilian investment. The institutional structure enabling this strategy is what Rich Marino describes as a "Socialist Market Economy" that maintains an incomplete transition to a market economy.[17] By bypassing conventional market mechanisms in favor of politically mandated Fixed Asset Investment–often used through State-Owned Enterprises and opaque financing vehicles – the PRC ensures its economic machinery remains fundamentally geared toward state-directed strategic goals.[18]

Shaomin Li provides the operational mechanism for this mobilization through the concept of China Inc., where the CCP has transformed the entire country into a giant corporation that eliminates the traditional boundary between government and private firm.[19] Under this system of "mobilizing the entire country" (*juguo tizhi,* 举国体制), infrastructure projects are not public works, but mandatory corporate directives executed by subsidiaries to achieve integration rather than reciprocity.[20]

Ultimately, China's economic model has undergone a crucial evolution under Chairman Xi Jinping. As Ian Murphy argues, the contemporary Beijing Consensus now explicitly prioritizes political security, regime stability, and ideological control over considerations of economic efficiency or social welfare.[21] This shift proves that when a perceived economic project, such as Kinmen's integration, is deemed essential for eliminating a challenge to the Party's authority, it ceases to be an economic venture and becomes a security imperative. Consequently, Kinmen's infrastructure projects function as the kinetic outcome of a calculated political-security operation, bridging the gap between induced economic dependency and the strategic goal of a non-kinetic *fait accompli*.

The Core-Periphery Imbalance

Within the localized cross-Strait context, dependency theory establishes the structural power imbalance where Kinmen County, as a resource-scarce territory, functions as a "periphery" to the massive economy and resource base of adjacent Xiamen. This core-periphery dynamic

identifies the structural vulnerability of Kinmen's water scarcity, creating a resource bottleneck that the mainland core is uniquely positioned to address at a relatively low cost. Consequently, this inherent disparity makes Kinmen an ideal candidate for targeted political integration through infrastructure development that leverages pre-existing structural weaknesses.

However, the PRC's approach in Kinmen inverts the traditional dependency paradigm, which emphasizes the extraction of wealth from the periphery to the core. Instead of exploitation, Beijing's strategy utilizes a calculated injection of resources and capital to generate political goodwill and functional dependency. This positive resource flow shifts the strategic objective from economic extraction toward political leverage and cognitive influence. Since these links are targeted strategic instruments of reunification, the analysis must move beyond general structural critique and toward frameworks that address the tactical deployment of economic tools for political incorporation.

The Use of Economic Tools: Economic Statecraft

Economic statecraft provides the operational framework for the Contested Kinmen Model, shifting the focus from structural vulnerability to the deliberate deployment of economic instruments for strategic ends. It shifts the focus from examining general structural vulnerability (as highlighted by Dependency Theory) to study the deliberate, calculated deployment of economic instruments to achieve strategic political goals. Blackwill and Harris define geoeconomics, which encompasses economic statecraft, as "the use of economic instruments to promote and defend national interests" and to produce beneficial geopolitical results through the cultivation of goodwill and compliance.[22]

This strategy functions as the first phase of a broader integration process: cultivating political affinity to lower resistance to long-term dependency. The New Four Links serve as prime examples of this positive statecraft, where tangible successes, such as the Jinjiang-Kinmen Water Pipeline, generate the political support necessary to advance more sensitive projects like the Kinmen-Xiamen Bridge. Thus, this statecraft is inseparable from cognitive warfare, as the PRC leverages infrastructure to manipulate local decision-making and incentivize residents to prioritize immediate developmental gains over long-term strategic autonomy. However, while economic statecraft describes the *intention* and the *tools*, it does not quantify the structural leverage inherent in the resulting network. To analyze how these induced dependencies are converted into coercive capacity, the analysis must move to the framework of Weaponized Interdependence.

Asymmetric and Weaponized Interdependence

Farrell and Newman's theoretical work on Weaponized interdependence challenges traditional liberal notions that interdependence necessarily fosters peace. Instead, it argues that structural power in a globalized world derives from controlling the asymmetric networks through which critical resources flow. This concept is defined as a condition where a central actor can intentionally leverage his political authority over hub nodes in an embedded network to gain asymmetric bargaining advantage over others. This network power operates through two primary coercive mechanisms: the *Panopticon Effect* (using network centrality to extract informational advantages) and the *Chokepoint Effect* (leveraging network centrality to cut adversaries off from network flows of information, goods, or capital).[23] Crucially, this potential for exploitation is not accidental but can be intentionally developed and accentuated by national policy to gain a strategic advantage.

While much of the initial analysis of weaponized interdependence focused on abstract networks like financial systems, such as SWIFT, the framework is profoundly relevant to physical critical infrastructure, such as utility pipelines and transportation links. The Kinmen infrastructure projects perfectly embody the creation of an infrastructural chokepoint. Cutting off access to vital, non-substitutable resources like freshwater is strategically analogous to disconnecting a nation from its financial payments system, which is considered the economic equivalent of crossing the nuclear threshold due to the near-complete lack of alternatives with comparable efficiency.[24] The water pipeline constitutes a centralized, single supply route for a non-fungible resource that Kinmen now heavily relies upon.

The high dependency metrics created by the water pipeline changes the Kinmen-Fujian relationship from mere economic inducement to a state of structural coercibility. While asymmetric interdependence refers to a general power imbalance, structural coercibility is the deliberate engineering of physical, non-substitutable chokepoints that grant an external actor the functional ability to dictate local policy by controlling essential resource flows. This represents a shift from a passive economic imbalance to an active, weaponized architecture designed to generate political compliance through infrastructure. Data from the Kinmen County Water Plant Statistical Yearbook reveals that water from coastal Fujian reached 70.9% of the island's total regular supply in 2022, far exceeding Taipei's political objective of limiting mainland dependency to 30%. On its current trajectory, the island is set to miss its target of 75% local sufficiency by 2031, cementing the pipeline as a primary vector of weaponized interdependence and a permanent lever of infrastructural coercion.

The 70.9 percent dependency metric provides empirical validation for the chokepoint effect, quantifying the success of the PRC's infrastructure statecraft. When dependence on an essential, non-substitutable resource crosses such a high threshold, the relationship becomes fundamentally asymmetric. The threat of disrupting this flow, whether overtly through political action or subtly through claimed "technical issues," becomes a permanently active political lever. The Kinmen case further expands the theoretical domain of weaponized interdependence application, as it involves tangible, physical critical infrastructure rather than abstract digital or financial networks. This physicality makes the coercive threat of the chokepoint vividly real and provides a robust, measurable case study for applying weaponized interdependence to strategic resource dependency in island territories or on the sub-national level.

The Kinmen strategy seeks to compound this vulnerability through the proposed multi-domain extension of the weaponized interdependence chokepoint. Preliminary technical preparations have been largely completed for electricity, natural gas, and bridge connections between coastal Fujian and Kinmen. If these proposed projects proceed, Kinmen's dependence will extend from a single critical domain (water) to multiple essential life domains (energy, transportation, access to services). This comprehensive asymmetric interdependence drastically increases coercive efficacy, making the island fully reliant on the mainland for economic and existential security, aligning perfectly with the goal of political incorporation. This deliberate creation of reliance facilitates cognitive warfare. The persistence of local support for PRC projects, despite obvious geopolitical risks, demonstrates a successful manipulation of local decision-making structures. By prioritizing the immediate resolution of developmental bottlenecks over long-term strategic autonomy, the PRC exploits local democratic processes and resource scarcity. The outcome is that the target population

and its leadership are incentivized to voluntarily enter the coercive network, supporting further integration and thereby eroding Taipei's effective control over the territory.

Theoretical Contribution

This article makes a distinct contribution to the study of irregular warfare and geoeconomics by expanding the framework of weaponized interdependence from global financial and digital networks into the realm of subnational physical infrastructure. While existing scholarship primarily analyzes *faits accomplis* through the lens of direct military seizure or maritime land reclamation, this study introduces the concept of infrastructural coercion to explain how ostensibly civilian development can institutionalize political control. By synthesizing these frameworks, this article provides a novel model for understanding how a revisionist power can achieve strategic incorporation through the creation of irreversible physical chokepoints, rather than kinetic conflict.

Methodology

The analysis uses a qualitative case study methodology focused on infrastructure that either connects the mainland with Kinmen County or PRC-initiated projects that will have a significant impact on Kinmen's governance. Kinmen serves as a high-leverage empirical case for understanding the PRC's strategy of non-kinetic infrastructural coercion aimed at achieving political objectives. Due to its unique geographic proximity and frontline status, Kinmen represents a visible, active theater where political change is actively shaped through infrastructure development. This study analyzes the PRC's actions within the definition of Irregular Warfare. The Department of Defense defines irregular warfare as a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. It often employs indirect, non-attributable, or asymmetric activities.

The PRC's strategic behavior concerning the Kinmen infrastructure projects is viewed against a contextual backdrop of heightened cross-strait tensions, including unilateral changes to air routes and increasing maritime incursions.[25] This synchronization suggests that infrastructure deployment is deliberately integrated alongside broader hybrid warfare tactics to achieve political objectives by Beijing. The core of this analysis utilizes weaponized interdependence, specifically the chokepoint effect as defined by Farrell and Newman, which offers the highest analytical precision for this set of cases. This framework shifts the focus from the process of influence (economic statecraft) to the mechanism of exploitation residing within the infrastructure network itself to create structural vulnerability. This framework is applied through two primary criteria of structural dependency and cognitive influence. This includes assessing how the infrastructure creates a centralized, single supply route for a non-substitutable resource, thereby forcing the island into a state of structural coercibility. Cognitive influence includes assessing how the positive resource flow is used to generate political leverage and influence local decision-making structures by prioritizing immediate, tangible benefits over long-term strategic autonomy.

The data analyzed consists of official policy documents, quantitative resource dependency metrics, and press releases from the Mainland Affairs Council in Taiwan. This is supplemented by media reports from both Taiwan and China. The case study focuses on the following key projects:

1. The operational Jinjiang-Kinmen Water Pipeline (2018),
2. The proposed Kinmen-Xiamen Bridge (proposed), and

3. Xiang'an Airport (under construction).

These cases serve as evidence of China's deliberate, long-term strategic institutional effort to put Kinmen, and thus Taiwan as a whole, in a state of structural coercibility. While critics may view these projects through the lens of liberal interdependence to characterize them as rational economic cooperation designed to meet Kinmen's legitimate developmental needs, the unilateral nature of the New Four Links and the engineering of irreversible chokepoints suggest that the coercion framework is more analytically accurate. By prioritizing the creation of structural vulnerability over mutual reciprocity, the PRC leverages these physical networks not as stabilizers, but as strategic instruments to achieve the functional and political incorporation of the target territory.

Case Study Analysis

The PRC's infrastructure deployment targeting Kinmen County is a calculated application of irregular warfare, defined by the Department of Defense as "a form of warfare where state and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities, either as the primary approach or in concert with conventional warfare."[26] These projects function as strategic instruments designed to achieve a non-kinetic *fait accompli*, utilizing civilian networks to bypass traditional diplomatic and military defenses.

The following analysis of the operational Jinjiang-Kinmen Water Pipeline, the proposed Kinmen-Xiamen Bridge, and the under-construction Xiamen Xiang'an Airport demonstrates how Beijing employs Altman's logic of "wresting territory," and the salami tactics that Richard Maass describes, to create irreversible strategic gains. By operationalizing weaponized interdependence, specifically the chokepoint effect, this approach shifts the focus from the process of influence to the mechanism of exploitation inherent in the infrastructure network itself. Collectively, these cases serve as evidence of a deliberate, long-term strategic effort to place Kinmen in a state of structural coercibility, effectively hollowing out democratic governance by presenting a completed reality of political incorporation.

Jinjiang-Kinmen Water Pipeline

First operational in 2018, the Jinjiang-Kinmen Water Pipeline represents a successful "limited *fait accompli*," where the PRC utilized a non-kinetic opening to wrest functional control over a resource essential for survival. As defined by Altman, this move denied Taipei the choice of whether to concede Kinmen's resource autonomy by presenting a completed physical reality that is now prohibitively costly to reverse. Spanning 28 kilometers, including a 16-kilometer undersea section from Jinjiang to Kinmen, the water pipeline addresses a critical need for freshwater previously met by unsustainable groundwater use, while simultaneously creating a permanent infrastructure chokepoint.[27] By linking Kinmen's survival directly to the mainland via this single supply route, the PRC bypassed traditional coercive threats, opting instead to capture a strategic gain that mimics the "weaponized interdependence" seen in other contested territories. Through bypassing coercive threats, this resource relationship can be likened to the dependencies established between Hong Kong and China or between the Crimean Peninsula and Russia prior to formal military operations in Ukraine.[28]

Figure B: Jinjiang-Kinmen Water Pipeline

Source: Kinmen County Water Plant, 2022.

*This map illustrates the route of the Jinjiang-Kinmen Water Pipeline (*圖 *3-3* 大陸引水海底輸水管線路徑圖*). The route starts at the Jinjiang (*晉江*) area in Fujian Province, connecting through several reservoirs: Dongshan Reservoir (*東山水庫*), Liangzhuo Reservoir (*溪邊水庫*), Longhu Reservoir (*龍湖*). The water is transported via land-based pipelines (black lines) on the mainland side and then crosses the sea via a 16.05km underwater pipeline (red line) from Dian Tou Bay (*圍頭灣*) to Tianpu (*田浦*) on Kinmen Island (*金門*).*

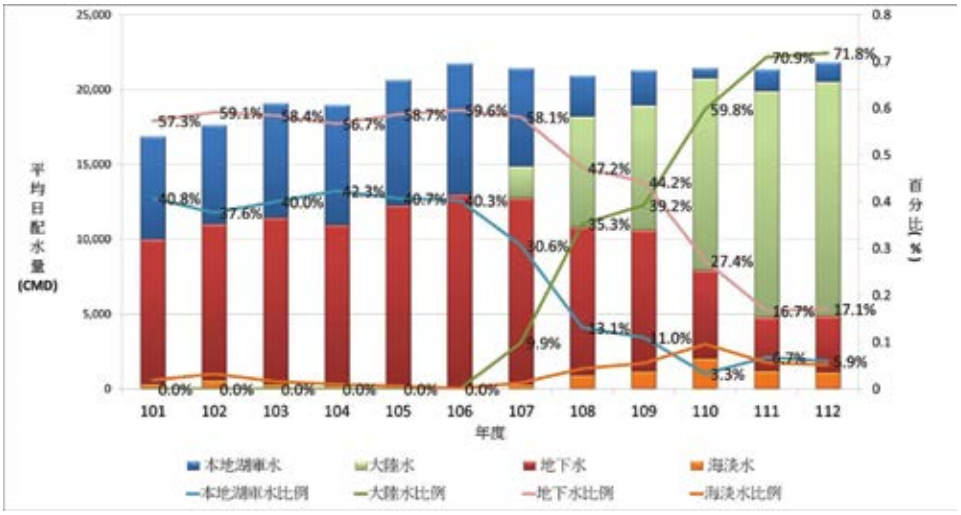
The reliance metrics validate this choke-point effect, functioning as a significant "slice" in a broader strategy of salami tactics. As Maass posits, such incremental *faits accomplis* are highly effective when executed in the shadow of a major war, as the target is deterred from escalating over a single, manageable revision to the status quo. By 2022 (ROC year 111), mainland water accounted for 70.9% of Kinmen's usage, while local groundwater reliance dropped to 16.7%.[29] This extreme dependency transforms a purely economic inducement into a state of structural coercibility, providing Beijing with a permanently active political lever. Additionally, the China Coast Guard's integration of pipeline "protection" into its patrol duties represents what Hastey identifies as the use of physical revisions to institutionalize control over contested space.[30] This intertwining of resource supply with maritime enforcement creates an irreversible material reality that anchors Kinmen's survival to mainland networks, rendering traditional notions of sovereignty increasingly secondary to functional integration.[31]

Beyond its structural advantage, the pipeline serves as a critical instrument of cognitive warfare, utilizing a positive resource flow to institutionalize a narrative of inevitable integration. By resolving the existential issue of water scarcity – an issue long neglected by the military-first postures of earlier eras–the PRC has created a material reality that Hastey identifies as the primary driver of political incorporation. This infrastructural *fait accompli* generates significant political goodwill, shifting local expectations toward mainland-led development and securing a complete reality in the minds of residents. The success of this maneuver lies in its ability to bypass coercive threats in favor of a tangible benefit that renders Taiwanese sovereignty appear increasingly abstract or even obstructive. Consequently, the PRC leverages this physical link to promote pro-unification narratives, framing the Xiamen-Kinmen Living Circle not as a choice, but as a geographical and logistical necessity.[32]

Kinmen-Xiamen Bridge

The Kinmen-Xiamen Bridge represents a definitive shift from negotiated functionalism to a unilateral *fait accompli* strategy. As the largest cross-strait

Figure C: Daily Water Supply For Kinmen



Source: Kinmen County Water Plant, 2022.

This chart displays the average daily water supply (平均日配水量, in cubic meters per day, CMD) for Kinmen over an 11-year period (Taiwanese Years 101 to 111, or 2012 to 2022). It illustrates the composition of the total water supply by source – local reservoir water, mainland China water, groundwater, and desalinated sea-water – and shows the corresponding percentage ratio for each source. Mainland Chinese water has risen from 0.0% (year 106 or 2017) to 70.9% (year 111 or 2022).

initiative within Xi Jinping's New Four Links, the project serves as a physical instrument designed to bypass the diplomatic rejection of Taiwan's Mainland Affairs Council. Unlike the water pipeline, which was the product of mutual negotiation, the bridge is being advanced through a strategy that Altman identifies as "wresting territory" by creating a completed reality that is prohibitively costly to reverse. The May 2024 completion of the A1 construction trestle – extending from Guanyinshan on Xiamen Island toward the Liuwudian Channel without Taipei's consent – denies the Taiwanese government the choice of whether to concede. Instead, this unilateral progress forces Taiwan to either accept the eventual physical link or initiate a disproportionately risky escalation to halt its advancement.[33]

The proposed bridge route would connect Kinmen directly to Xiamen via the Xiang'an International Airport – a mega-infrastructure project currently under construction on reclaimed land near Kinmen.[34] The bridge, however, cannot be fully completed without the formal assent of the Taiwan government. Depending on the final route (6km to 11km), the project was estimated to cost up to NT$13.2 billion (US$413.46 million, 2023 exchange rate).[35] The PRC currently has planned four distinct routes for the Kinmen-Xiamen Bridge. Routes 1, 2, and 3 propose connecting Xiamen's Wulao Mountain (五老山) area with Dadeng Island (大嶝) and Xiaodeng Island (小嶝), with varying lengths and estimated costs (in RMB). Route 4 is a conceptual extension from Dajinmen (大金門) to Xiaojinmen (小金門) and then to Xiamen Island.[36]

Taiwan's government has consistently rejected the project, viewing it as a unilateral political tactic by the CCP. In addition to labeling this project as a 'Trojan horse,' the Mainland Affairs Council argues that, unlike the Mini Three Links, the current regional situation is defined by the CCP's policy shift toward maximum intimidation and suppression. As such, Taiwan's government maintains that there are no policies or plans to facilitate the construction of a bridge between Kinmen and Xiamen and directly asks all sectors of Taiwan's society to not "dance to the CCP's tune."[37]

The bridge project is designed to institutionalize structural dependency and enhance the vulnerability of Kinmen, thereby increasing Beijing's coercive leverage. The Kinmen-Xiamen bridge would create a permanent physical link that would cement Kinmen's reliance on the PRC's infrastructure, economic, and security network. This would extend the PRC's existing infrastructure and bureaucratic institutional penetration of Kinmen. Outside of a wartime context, the bridge project strengthens the CCP's jurisdictional argument that Kinmen residents should have the same protection under PRC law as PRC citizens. Mainland Chinese media sources have already claimed that Kinmen's fishermen are under threat from Taiwan and require protection by the Chinese Coast Guard, equating legal Taiwanese citizens to citizens of the PRC.[38]

At the same time, the PRC has been promoting a tiered resident card system for Taiwanese citizens. PRC travel permits, residential permits, settlement certificates, and PRC ID cards offer varying levels of inducements to Taiwanese citizens, from opening social media accounts on Chinese platforms to looser travel restrictions within mainland China and even the ability to take out loans from Chinese banks.[39] Despite it being illegal for Taiwanese citizens to obtain PRC ID cards, there are few countermeasures for Taiwan to directly take against the PRC for the incremental "passportization" of its citizens. This "passportization" strategy will only pick up in intensity as physical and bureaucratic links bind Taiwan's territories and its citizens closer to the PRC.

In the event of a war, if a bridge were constructed, it would eliminate the natural barrier of the Taiwan Strait, allowing the People's Liberation Army to directly access the island. A Democratic Progressive Party lawmaker likened the risk to the Russo-Ukrainian war, where land connection allowed Russia to "drive straight into Ukrainian territory."[40] If the PLA initiates a military blockade or anti-access area denial against Taiwan's main island – a highly probable form of military pressure – flights and maritime transport from Taiwan to Kinmen would be unable to operate. In this event, Kinmen's survival would depend on the infrastructure "umbilical cord" connecting it to China.[41] This infrastructure becomes the ultimate chokepoint, giving China complete control over the island's functioning, allowing Kinmen to be isolated without the PLA firing a shot.

For the time being, China wields the Kinmen-Xiamen bridge project primarily as a tool for cognitive warfare, aiming to manipulate the thought processes, behavior, and political loyalties of the Kinmen populace to facilitate its peaceful annexation. The project generates goodwill by addressing practical, critical needs that the Taiwan government has struggled to meet adequately. Local residents and politicians supportive of the bridge point out that it would significantly address essential livelihood issues, including improving local healthcare, solving waste disposal problems, and providing access to stable electricity and natural gas. Residents specifically desire rapid access to the more advanced medical facilities available in Xiamen.[42] The bridge is promoted as an "economic lifeline" that would link Kinmen to the far larger Xiamen market, creating job opportunities and boosting the tourism economy, which is already dependent on PRC

visitors.[43] Kinmen residents thus may feel integration is a geographical necessity.

The CCP leverages the bridge as a powerful inducement to fragment Taiwan's political discourse, transforming a civil engineering project into a cognitive wedge. By portraying the bridge as a foundational "steppingstone" for a "Cross-Strait Peace Experimental Zone," Beijing effectively frames political incorporation as a prerequisite for local prosperity. This strategy has successfully co-opted local political actors, such as Taiwan People's Party Chairman Ko Wen-je and various Kuomintang candidates, who have amplified CCP narratives by championing "Kinmen First" platforms and "pilot economic zones."[44] As Altman notes, the strategic power of such a *fait accompli* lies in its ability to force an opponent to engage with a new reality on the aggressor's terms. By compelling mainstream Taiwanese parties to respond to these localized infrastructure demands, the PRC successfully operationalizes salami tactics, thus creating deep internal divisions that hollow out national consensus while presenting integration as a geographical and logistical inevitability.

Xiamen Xiang'an International Airport

The Xiamen Xiang'an International Airport represents a distinct escalation in the PRC's use of infrastructure as irregular warfare, shifting from the negotiated dependency of the water pipeline to a strategy of unilateral spatial and sovereign encroachment. Although officially framed by Beijing as a pivotal regional hub, the airport is strategically positioned to physically and operationally subsume Kinmen into the PRC's transportation network and is thus designed to wrest territory by creating a physical reality that is prohibitively costly to reverse. Unlike the bridge proposal, which remains a political lever requiring Taiwanese consent, the airport is actively being constructed to irreversibly alter the geopolitical geography of the Taiwan Strait. This section analyzes how the project employs physical revisions to the status quo by using environmental engineering, air traffic dominance, and market gravity to enforce the Xiamen-Kinmen Living Circle and erode Taiwan's air defense buffer.

The airport is being built in the Xiang'an District of Xiamen City. Specifically, it is located on reclaimed land at Dadeng Island (大嶝島) and Xiaodeng Island (小嶝島) in the Southeastern Sea area of Dadeng Island. The location is about 25km (straight-line distance) from the center of Xiamen City. The project involves massive land reclamation, with a total of 25.58sq km of land being reclaimed between 2010 and 2020.[45] This reclamation has had a significant geopolitical effect by reducing the distance between the mainland and Kinmen from approximately six kilometers to three kilometers.[46]

The planning of the Xiang'an Airport began in 2007, with the feasibility study report for the project officially approved by China's National Development and Reform Commission in April 2021.[47] Construction of the main terminal building began in 2022. The airport is expected to be operational in 2026, replacing the existing Xiamen Gaoqi International Airport as Xiamen's main aviation hub. The first phase is designed to meet the annual target of 45 million passengers and 750,000 tons of cargo. It features a terminal building of 550,000sq meters, two runways (one 3,800m runway built to 4F standard and one 3,600m runway built to 4E standard), and 196 aircraft parking bays.[48] By 2040, the airport is projected to serve 85 million passengers and two million tons of cargo annually.[49]

The Xiamen Xiang'an International Airport is being built not solely for civilian needs, but as a multi-layered strategic investment tied directly to Beijing's political and integration goals of Taiwan. The airport is officially marketed as a pivotal regional airport, part of the Belt and Road Initiative, and a cross-strait exchange gateway.[50] It is explicitly

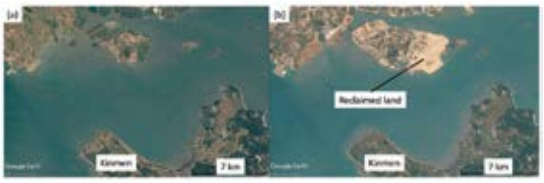
designed as part of the transportation network for the proposed Xiamen-Kinmen Life Circle. As part of the New Four Links, the political intent is to connect Kinmen to the new airport and share its use with Kinmen residents.

The airport is promoted as a means of addressing capacity constraints, enhancing regional connectivity, and fostering economic development in the region, including the promotion of air cargo logistics and aviation-related technological innovation.[51] PRC media also frames the airport and its related infrastructure projects as stepping stones towards integrating Kinmen – and later all of Taiwan – under PRC control.[52] The construction of such a mega-airport demonstrates the modernization and economic development capabilities of the CCP, which is then leveraged to promote the regime's economic governance model and legitimize its political control.[53] Materially, there are four specific threats that will only increase in severity as time goes on: the threat of land reclamation, the disruption of air traffic, the monopolization of air traffic, and even the future wartime conversion of the airport into a military hub.

China's Proximity and the Threat of Land Reclamation

Kinmen's geographical proximity to the Chinese mainland is already profound, with the North-facing shores of the archipelago offering a direct view of Xiamen's skyscrapers and port infrastructure. However, satellite imagery confirms that the massive land reclamation for the Xiang'an Airport is halving the distance between Kinmen and the mainland from six kilometers to just three. This deliberate act of environmental engineering represents yet another physical revision to the status quo, this time institutionalizing PRC control over a combination of land, maritime, and airspace. This land reclamation serves as a strategic *fait accompli* that irreversibly alters the physical environment in China's favor, creating a new material reality that renders traditional maritime boundaries and air defense buffers increasingly obsolete.[54]

Figure G: Satellite Image Of Xiamen Airport Land Reclamation



Source: Tu and Huang, 2023

Satellite images illustrate the impact of land reclamation for the Xiamen Xiang'an Airport project. Figure (a) shows the coastal area near Xiamen and Kinmen in December 2010, before significant reclamation. Figure (b) shows the same area in December 2020, with a large area of reclaimed land clearly visible. These images highlight the dramatic environmental and geographical changes brought about by the construction of infrastructure projects like Xiang'an Airport.

Land reclamation projects like the Xiang'an Airport, and China's militarized South China Sea artificial islands, require large amounts of sand. It is possible that these land reclamation projects are connected to illegal sand dredging by Chinese vessels near Taiwan's Matsu Islands. The sand "stealing" is widely considered by Taiwanese officials and military analysts to be a non-military form of warfare designed to harass, intimidate residents, and damage the local economy and environment, and exhaust Taiwan's limited defense resources without triggering open conflict. The dredging activities have also repeatedly damaged undersea communication cables connecting Matsu to the main island of Taiwan, causing internet and phone outages.[55] The illegal mining destroys seabed habitats, causes coastal erosion, and depletes marine life, severely

impacting the livelihoods of Taiwanese fishermen and the ecosystem.[56] It is likely that the sand being dredged from around Taiwan's outlying islands is being diverted for mega-projects like the Xiang'an Airport's land reclamation, used to make concrete for these projects, and being used to build military bases in the South China Sea, all while eroding the ecosystems, economy, and the defense of Taiwan's outlying islands.

Air Traffic Disruption

The way that the PRC has been going about constructing the airport and designing air routes poses a threat to Taiwan's aviation safety and sovereignty by increasing air traffic congestion near Taiwanese routes and lack of consultation with Taiwanese authorities. The lack of consultation over the expansion of China's civilian air routes significantly heightens the risk of accidents through miscommunication.[57] The Civil Aviation Administration of China has been expanding and relocating civil aviation flight paths in the Taiwan Strait unilaterally. Notably, the expansion of the W122 and W123 routes to allow eastbound flights means that traffic now operates in close proximity to existing Taiwanese civilian flight routes – particularly W2, W6, and W8 – which connect the outlying islands of Kinmen and Matsu to Taiwan's main island.[58]

The massive scale and strategic positioning of Xiang'an International Airport create a plausible risk scenario in which Kinmen's existing Shangyi Airport is economically and operationally subsumed. By establishing the mega-airport as the primary portal for cross-strait exchange, Beijing denies Taipei the choice of maintaining autonomous external connectivity. This infrastructural monopoly allows the Chinese Communist Party to leverage unspoken threats to flight safety as a permanent active political lever, where any incident could be weaponized to discredit democratic governance and justify unilateral maritime and aviation enforcement.

This spatial encroachment also facilitates a deeper form of Hastey's institutionalized control through the mandatory application of Chinese domestic law. The extraterritorial reach of the 2020 National Security Law suggests a scenario where Taiwanese passengers transiting through Xiang'an could be subject to arbitrary detention or exit bans for activities that occurred outside of PRC jurisdiction.[59] In essence, should Shangyi Airport become unviable, Kinmen's survival would necessitate transit through mainland China, completing an infrastructural *fait accompli*. In this scenario, Kinmen would be rendered irreversibly beholden to the CCP, as its residents are functionally integrated into the mainland's legal and political jurisdiction through the very infrastructure intended for their connectivity.

Conclusion

The emergence of the "Contested Kinmen Model" signifies a profound shift in cross-strait relations, where the PRC has successfully weaponized civilian infrastructure to bypass traditional diplomatic defenses. By transitioning from the negotiated, cooperative framework of the Mini Three Links to the unilateral imposition of the New Four Links, Beijing has operationalized a strategy of irregular warfare that targets the structural foundations of Kinmen's society. The case studies of the Jinjiang-Kinmen Water Pipeline, the Kinmen-Xiamen Bridge, and Xiang'an Airport demonstrate that these projects are not merely developmental initiatives, but calculated mechanisms of weaponized interdependence designed to establish permanent strategic chokepoints. The operational water pipeline already serves as an established chokepoint that has enabled increased PRC gray zone activities, providing the foundation for expanding this model across the Taiwan Strait.

Ultimately, these infrastructure mega-projects function as a non-kinetic means to achieve a *fait accompli* of political incorporation, rendering the physical boundary of the Taiwan Strait increasingly irrelevant. Following Dan Altman's logic of wresting territory, Beijing utilizes these physical networks to deny Taipei the choice of whether to concede, presenting a completed reality that is prohibitively costly to reverse. This cumulative expansion is achieved through salami tactics, where incremental, sub-conflict revisions erode Taipei's effective sovereignty by manipulating local cognitive vulnerabilities. If the bridge and airport projects proceed as intended, the PRC will use physical revisions to effectively subsume Kinmen into the PRC's logistical and legal jurisdiction, isolating the outlying islands from Taiwan's defense perimeter without a single shot being fired.

Beyond the Taiwan Strait, the Kinmen Model serves as a strategic blueprint for the PRC's broader global engagement through the Belt and Road Initiative and maritime expansion. By utilizing subnational infrastructure to create irreversible physical markers of authority, Beijing can effectively export this model of infrastructural coercion to other contested regions. This approach demonstrates how revisionist powers can achieve strategic incorporation through the creation of physical chokepoints and cognitive dependencies, hollowing out democratic governance from within long before conventional military conflict is ever initiated.

Endnotes

[1] Murphy, Ian. "Securitizing Kinmen: China's Gray Zone Strategy and the Evolution of the Kinmen Model." *Inter Populum Journal of Irregular Warfare and Special Operations* Fall 2025 (November 2025). https://interpopulum.org/securitizing-kinmen-chinas-gray-zone-strategy-and-the-evolution-of-the-kinmen-model/.

[2] Ian Murphy. "China's Infrastructure Warfare Against Kinmen." *Taiwan Insight*, June 7, 2024. https://taiwaninsight.org/2024/06/07/chinas-infrastructure-warfare-against-kinmen/.

[3] Mainland Affairs Council. *MAC Solemnly Rejects the Claim That "a Kinmen-Xiamen Bridge Is a Policy Continuation of the 'Mini Three Links'" and Calls for National Security to Be Prioritized When Promoting Cross-Strait Affairs*. News Release Report No. 007. Mainland Affairs Council, 2022. https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&sms=E828F60C4AFBAF90&s=7C5D17646E80A429.

[4] Cheng-fung Lu. "China Initiates a New Integration Model with Taiwan, Starting with Gray Zone Tactics towards Kinmen." *Global Taiwan Brief* 7, no. 17 (2022). https://globaltaiwan.org/2022/08/china-initiates-a-new-integration-model-with-taiwan-starting-with-gray-zone-tactics-towards-kinmen/.

[5] Liu Shenkui (劉深魁). "小三通"开通二十年 累计运送旅客超2208万人次 [Twenty Years of the 'Mini Three Links': Over 22.08 Million Passengers Transported in Total]." *Renmin Ribao Haiwai Ban (人民日报海外版) [People's Daily Overseas Edition]*, January 12, 2021. http://tw.people.com.cn/n1/2021/0112/c14657-31996984.html.

[6] Cheng-fung Lu. "China Initiates a New Integration Model with Taiwan, Starting with Gray Zone Tactics towards Kinmen." *Global Taiwan Brief* 7, no. 17 (2022). https://globaltaiwan.org/2022/08/china-initiates-a-new-integration-model-with-taiwan-starting-with-gray-zone-tactics-towards-kinmen/.

[7] Murphy, Ian. "Securitizing Kinmen: China's Gray Zone Strategy and the Evolution of the Kinmen Model." *Inter Populum Journal of Irregular Warfare and Special Operations* Fall 2025 (November 2025). https://interpopulum.org/securitizing-kinmen-chinas-gray-zone-strategy-and-the-evolution-of-the-kinmen-model/.

[8] Xi Jinping. "Working Together to Realize Rejuvenation of the Chinese Nation and Advance China's Peaceful Reunification." Meeting Marking the 40th Anniversary of the Issuance of the Message to Compatriots in Taiwan. 中共中央台湾工作办公室、国务院台湾事务办公室 (Taiwan Affairs Office of the Central Committee of the Communist Party of China, Taiwan Affairs Office of the State Council). Beijing, January 2, 2019. http://www.gwytb.gov.cn/wyly/201904/t20190412_12155687.htm.

[9] Eric Chan. "The Coming Systems Confrontation over Kinmen." *Global Taiwan Brief* 6, no. 5 (2021). https://globaltaiwan.org/2021/03/the-coming-systems-confrontation-over-kinmen/.

[10] Ian Murphy and Eric Chan. "Countering Cognitive Warfare: Taiwan's Defense Against Party Influence in Kinmen." *Global Taiwan Brief* 9, no. 14 (2024). https://globaltaiwan.org/2024/07/countering-cognitive-warfare-taiwans-defense-against-party-influence-in-kinmen/.

[11] Mainland Affairs Council. *MAC Solemnly Rejects the Claim That "a Kinmen-Xiamen Bridge Is a Policy Continuation of the 'Mini Three Links'" and Calls for National Security to Be Prioritized When Promoting Cross-Strait Affairs*. News Release Report No. 007. Mainland Affairs Council, 2022. https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&sms=E828F60C4AFBAF90&s=7C5D17646E80A429.

[12] Mainland Affairs Council. *MAC Solemnly Rejects the Claim That "a Kinmen-Xiamen Bridge Is a Policy Continuation of the 'Mini Three Links'" and Calls for National Security to Be Prioritized When Promoting Cross-Strait Affairs*. News Release Report No. 007. Mainland Affairs Council, 2022. https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&sms=E828F60C4AFBAF90&s=7C5D17646E80A429.

[13] Altman, Dan. "By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries." *International Studies Quarterly* 61, no. 4 (2017): 881–91. https://doi.org/10.1093/isq/sqx049.

[14] Maass, Richard W. "Salami Tactics: Faits Accomplis and International Expansion in the Shadow of Major War." *Texas National Security Review* 5, no. 1 (2021): 34–54.

[15] Hastey, Joshua. *China, Faits Accomplis and the Contest for East Asia*. Routledge Studies in Foreign Policy Analysis. Routledge, 2023.

[16] Ramo, Joshua Cooper. "The Beijing Consensus." *The Foreign Policy Centre*, 2004. Page 2.

[17] Marino, Rich. *The Evolution of China's Political Economy*. Routledge, 2023. Page 16.

[18] Marino, Rich. *The Evolution of China's Political Economy*. Routledge, 2023.

[19] Li, Shaomin. *The Rise of China, Inc.: How the Chinese Communist Party Transformed China into a Giant Corporation*. Cambridge University Press, 2022.
[20] Li, Shaomin. *The Rise of China, Inc.: How the Chinese Communist Party Transformed China into a Giant Corporation*. Cambridge University Press, 2022. Page 130.
[21] Murphy, Ian. "The Evolving Beijing Consensus: CCP Political Control and Economic Tradeoffs." *Journal of Geoeconomics*, forthcoming.
[22] Blackwill, Robert D., and Jennifer M. Harris. *War by Other Means: Geoeconomics and Statecraft*. Belknap Press of Harvard University Press, 2016.
[23] Farrell, Henry, and Abraham L Newman. "Weaponize Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44, no. 1 (2019): 42–79. https://doi.org/10.1162/ISEC_a_00351.
[24] Farrell, Henry, and Abraham L Newman. "Weaponize Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44, no. 1 (2019): 42–79. https://doi.org/10.1162/ISEC_a_00351.
[25] Hsia, Hsiao-hwa, and Tsung-han Lee. "Taiwan's Kinmen Island: On the Front Lines of Tension with China." *Radio Free Asia*, March 27, 2025. https://www.rfa.org/english/news/china/kinmen-island-taiwan-tensions-03272024133330.html.
[26] Robert Schafer, Martijn Kitzen, Peter Layton, et al. "Understanding Irregular Warfare." *Center for Army Lessons Learned* 25–897 (July 2025). https://www.army.mil/article/286976/understanding_irregular_warfare#:~:text=The%20Department%20of%20Defense%20(DOD)%20defines%20irregular,armed%20violence**%20*%20**Nonmilitary%20sources%20of%20power**.
[27] 金門縣自來水廠 Kinmen County Water Plant. 金門縣自来水廠統計年報：中華民國*111*年 *Kinmen County Water Plant Statistical Yearbook*. December 2022.
[28] 金門縣自來水廠 Kinmen County Water Plant. 金門縣自来水廠統計年報：中華民國*111*年 *Kinmen County Water Plant Statistical Yearbook*. December 2022.
[29] 金門縣自來水廠 Kinmen County Water Plant. 金門縣自来水廠統計年報：中華民國*111*年 *Kinmen County Water Plant Statistical Yearbook*. December 2022.
[30] Wang Qi. "Fujian Coast Guard Conducts Routine Patrol in Waters near Kinmen, 'Safeguarding Maritime Homeland Security, Fishing Interests.'" *Global Times*, May 8, 2024. https://www.globaltimes.cn/page/202405/1311919.shtml.
[31] 金門縣自來水廠 Kinmen County Water Plant. 金門縣自来水廠統計年報：中華民國*111*年 *Kinmen County Water Plant Statistical Yearbook*. December 2022.
[32] Ian Murphy and Eric Chan. "Countering Cognitive Warfare: Taiwan's Defense Against Party Influence in Kinmen." *Global Taiwan Brief* 9, no. 14 (2024). https://globaltaiwan.org/2024/07/countering-cognitive-warfare-taiwans-defense-against-party-influence-in-kinmen/.
[33] Chen Yu-fu and Jason Pan. "Kinmen Bridge Plan Slammed over Security Fears." Taipei Times, August 24, 2023. https://www.taipeitimes.com/News/taiwan/archives/2023/08/24/2003805214.
[34] Chen Yu-fu and Jason Pan. "Kinmen Bridge Plan Slammed over Security Fears." *Taipei Times*, August 24, 2023. https://www.taipeitimes.com/News/taiwan/archives/2023/08/24/2003805214.
[35] Dot Dot News. "金門大橋通車 5分鐘車程走了30年" [Kinmen Bridge Opens to Traffic: A 5-Minute Drive Took 30 Years]." 點新聞 [Dot Dot News], November 1, 2022. https://www.dotdotnews.com/a/202211/01/AP636093a5e4b0adad9d65fc96.html.
[36] Dot Dot News. "金門大橋通車 5分鐘車程走了30年" [Kinmen Bridge Opens to Traffic: A 5-Minute Drive Took 30 Years]." 點新聞 *[Dot Dot News]*, November 1, 2022. https://www.dotdotnews.com/a/202211/01/AP636093a5e4b0adad9d65fc96.html.
[37] Mainland Affairs Council. *MAC Solemnly Rejects the Claim That "a Kinmen-Xiamen Bridge Is a Policy Continuation of the 'Mini Three Links'" and Calls for National Security to Be Prioritized When Promoting Cross-Strait Affairs*. News Release Report No. 007. Mainland Affairs Council, 2022. https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&sms=E828F60C4AFBAF90&s=7C5D17646E80A429.
[38] Murphy, Ian. "Securitizing Kinmen: China's Gray Zone Strategy and the Evolution of the Kinmen Model." *Inter Populum Journal of Irregular Warfare and Special Operations* Fall 2025 (November 2025). https://interpopulum.org/securitizing-kinmen-chinas-gray-zone-strategy-and-the-evolution-of-the-kinmen-model/.
[39] Sze-Fung Lee. "PRC ID Cards and Hybrid Warfare: The Accumulated Impact on Taiwan and Potential Countermeasures." *Global Taiwan Brief* 10, no. 11 (2025). https://globaltaiwan.org/2025/06/prc-id-cards-and-hybrid-warfare/.
[40] Eric Cheung, Will Ripley, and John Mees. "A China-Taiwan DMZ? Meet the Kinmen Islanders Who Want a Bridge, Not a War." *CNN*, June 1, 2023. https://www.cnn.com/2023/06/01/asia/taiwan-china-tensions-kinmen-island-dmz-intl-hnk/index.html.
[41] Ian Murphy. "China's Infrastructure Warfare Against Kinmen." *Taiwan Insight*, June 7, 2024. https://taiwaninsight.org/2024/06/07/chinas-infrastructure-warfare-against-kinmen/.

[42] Brian Hioe. "With Kinmen Comments, Ko Wen-Je Dives Into Cross-Strait Debate." *The Diplomat*, July 1, 2022. https://thediplomat.com/2022/07/with-kinmen-comments-ko-wen-je-dives-into-cross-strait-debate/.
[43] Sarah Wu. "Bridge Dilemma Captures Divide over China in Taiwan Elections." *Reuters*, January 10, 2024. https://www.reuters.com/world/asia-pacific/bridge-dilemma-captures-divide-over-china-taiwan-elections-2024-01-09/.
[44] Sarah Wu. "Bridge Dilemma Captures Divide over China in Taiwan Elections." *Reuters*, January 10, 2024. https://www.reuters.com/world/asia-pacific/bridge-dilemma-captures-divide-over-china-taiwan-elections-2024-01-09/.
[45] Min-cheng Tu and Yu-chieh Huang. "Impact of Land Reclamation on Coastal Water in a Semi-Enclosed Bay." *Remote Sensing* 15, no. 2 (2023). https://doi.org/doi.org/10.3390/rs15020510.
[46] 搜狐公司 [Sohu]. 厦门将有大动作，两岸土地距离变近，台军头态度变软要找大陆协商 *[Xiamen Is Set to Make a Major Move, Bringing the Land Distance between the Two Sides of the Taiwan Strait Closer, and Taiwanese Military Leaders Are Softening Their Stance and Seeking Negotiations with the Mainland]*. June 15, 2024. https://www.sohu.com/a/785607715_121450515?scm=10004.442699_15-300022.0.10126.1101.top-ic:442699:110078.0.11.a2_5X14X40&spm=smpc.home.author-subscribe.4.1718452770134PiIvJ9L_1467.
[47] 郭泷钰 [Guo Longyu] and 邹玨 [Zou Hong]. "厦门新机场工程项目可行性研究报告正式获国家批复 [The Feasibility Study Report for the Xiamen New Airport Project Has Been Officially Approved by the State.]." 东南网 *[Southeast Network]*, April 30, 2021. https://xm.fjsen.com/2021-04/30/content_30715939.htm.
[48] 郭泷钰 [Guo Longyu] and 邹玨 [Zou Hong]. "厦门新机场工程项目可行性研究报告正式获国家批复 [The Feasibility Study Report for the Xiamen New Airport Project Has Been Officially Approved by the State.]." 东南网 *[Southeast Network]*, April 30, 2021. https://xm.fjsen.com/2021-04/30/content_30715939.htm.
[49] Schindler Management Ltd. *Xiamen Xiang'an International Airport*. February 4, 2024. https://group.schindler.com/en/media/stories/xiamen-xiangan-international-airport.html.
[50] Schindler Management Ltd. *Xiamen Xiang'an International Airport*. February 4, 2024. https://group.schindler.com/en/media/stories/xiamen-xiangan-international-airport.html.
[51] Schindler Management Ltd. *Xiamen Xiang'an International Airport*. February 4, 2024. https://group.schindler.com/en/media/stories/xiamen-xiangan-international-airport.html.
[52] Murphy, Ian. "Securitizing Kinmen: China's Gray Zone Strategy and the Evolution of the Kinmen Model." *Inter Populum Journal of Irregular Warfare and Special Operations* Fall 2025 (November 2025). https://interpopulum.org/securitizing-kinmen-chinas-gray-zone-strategy-and-the-evolution-of-the-kinmen-model/.
[53] Murphy, Ian. "The Evolving Beijing Consensus: CCP Political Control and Economic Tradeoffs." *Journal of Geoeconomics*, forthcoming.
[54] Min-cheng Tu and Yu-chieh Huang. "Impact of Land Reclamation on Coastal Water in a Semi-Enclosed Bay." Remote Sensing 15, no. 2 (2023). https://doi.org/doi.org/10.3390/rs15020510.
[55] Reuters. "Taiwan Activates Back-up Communication for Matsu Islands after Undersea Cables Malfunctioned." *Reuters*, January 21, 2025. https://www.reuters.com/world/asia-pacific/taiwan-digital-ministry-says-undersea-cables-matsu-islands-are-disconnected-2025-01-22/#:~:text=Disruptions%20to%20undersea%20cables%20have,balloon%20overflights%20and%20sand%20dredging.&text='Taiwan%2C%20which%20China%20views%20as,for%20remote%20areas%20including%20Matsu.
[56] Yimou Lee. "China's Latest Weapon against Taiwan: The Sand Dredger." *Reuters*, February 5, 2001. https://www.reuters.com/graphics/TAIWAN-CHINA/SECURITY/jbyvrnzerve/#:~:text=The%20ploy%20is%20taxing%20for,is%20destroying%20marine%20life%20nearby.
[57] Thomas Shattuck. "China's New Civil Flight Routes: Implications for Cross-Strait Stability." *Global Taiwan Brief* 9, no. 5 (2024). https://globaltaiwan.org/2024/03/chinas-new-civil-flight-routes-implications-for-cross-strait-stability/.
[58] 交通部民用航空局 [Ministry of Transportation and Communications, Civil Aeronautics Administration]. 中國片面改變M503航路飛行偏置等相關措施，已影響飛行安全，交通部民航局嚴正抗議並要求儘速協商 [China's Unilateral Change to M503 Route Flight Offset and Other Related Measures Has Affected Flight Safety; CAA Seriously Protests and Demands Expedited Consultation]. 2024. https://www.caa.gov.tw/News-Publish-Content.aspx?lang=1&nid=2283&a=381&ssd=2023/02/28&sed=2024/02/28&title=&ngid=1.
[59] U.S. Department of State, "Hong Kong International Travel Information," International Travel, last modified January 21, 2025. https://travel.state.gov/content/travel/en/international-travel/International-Travel-Country-Information-Pages/HongKong.html#:~:text=Once%20you%20pass%20through%20the,detention%2C%20expulsion%2C%20or%20prosecution.

Defending with One Hand

How U.S. Cyber Policy Constrains Private Cyber Defense

By Dr. Mark Grzegorzewski and Tanner Tunstall

Introduction

Private U.S. firms operate on the frontline of persistent competition in cyberspace against capable cyber actors, including those linked to China and Russia. This competition occurs daily, yet U.S. private industry lacks legal authorities that would allow it to respond in such a way as to impose costs on those actors. As a result, foreign non-government actors face little incentive to refrain from exploiting U.S. private-sector targets, actions that gradually erode U.S. national power. These activities take advantage of seams within the United States, targeting where national security responsibilities end, and private-sector obligations begin. American laws governing public–private defense relationships have created an asymmetric advantage in cyberspace for U.S. adversaries, enabling foreign actors to exploit U.S. private infrastructure with limited resistance.

This asymmetry is reinforced by a self-imposed and inflexible policy framework that constrains U.S. responses while adversaries operate with fewer internal limitations. In many cases, those adversaries employ non-governmental cyber actors, drawing on all elements of their societies, public and private, legal and illegal, to compete against the U.S. by targeting its private firms. By contrast, the United States relies primarily on

Dr. Mark Grzegorzewski is an Assistant Professor of Cybersecurity at Embry Riddle Aeronautical University. Dr. Grzegorzewski worked for the Department of Defense more than 13 years, eight of those years at U.S. Special Operations Command (SOCOM). During that time, he developed the first cyber curricula for USSOCOM and served as a Joint Special Operations Senior Fellow focused on cyberspace activities and operations. He is also Global and National Security Institute Fellow.

Tanner Tunstall is a Crisis Response Technology Coordinator at Sibylline Ltd. He earned a B.S. in Homeland Security from Embry-Riddle Aeronautical University, with minors in Cybersecurity Applications & Management and Aviation. His professional work centers on crisis intelligence, incident management, and mass notification platforms, and the integration of technical systems to support security, resilience, and emergency response operations, including applied cybersecurity, geospatial tools, and complex operational risk environments.

overstretched military cyber forces to project offense capabilities, while defending the perimeter against nation-state–level threats. These U.S. forces are focused on strategic missions, which have the effect of treating intrusions into U.S. private networks with lower priority or even going unanswered in the near term. These delays unintentionally shape expectations about what constitutes acceptable targeting behavior in cyberspace and can encourage continued or expanded exploitation.

This article argues the U.S. should untie the other hand of cybersecurity firms by expanding the authorities of verified, capable private cybersecurity firms to dial-up active defense measures to a metaphorical "stun" level, equivalent to not allowing attackers access to their own systems in response to a breach. Such authorities would enable these firms to restrict adversaries access to vulnerable systems, impose tangible costs on private malign actors, and enhance the overall resilience of the U.S. private sector. This would involve bringing private U.S. cyber hack-back capability out of the shadows and putting it to work to more effectively instill doubt in the mind of the attacker.[1] Doing so would require a shift from the prohibition of hacking back toward a controlled authorization of private cyber activity.[2]

Instead of criminalizing hack-back activity that already occurs, the United States should effectively empower qualified private cybersecurity firms by loosening legal constraints, enabling them to operate within a clear legal framework that explicitly does not connect them to the state.[3] Doing so would strengthen deterrence, improve predictability in cyberspace through transparency, and reduce risk to U.S. private industry, which is persistently targeted. Private hack-back actors have existed since the early days of the Internet, and their actions have not led to uncontrolled escalation. It is therefore time to be intellectually honest about the cyberspace environment, accept it as it exists, and take corrective action by authorizing and unleashing U.S. private cybersecurity capability to protect American private industry from foreign non-governmental actors.[4]

In making this claim, we first demonstrate how U.S. cyber policy rests on outdated assumptions that sharply separate public and private authority. Drawing on international cases and two decades of cyber incidents, we find little public evidence that private or hybrid cyber activity leads to uncontrollable escalation, despite persistent policy concerns about attribution, risk, and loss of control. We then argue that existing law, particularly the Computer Fraud and Abuse Act (CFAA), makes legislative reform unlikely in the near term. We conclude with narrowly tailored Department of Justice guidance to authorize tightly controlled private-sector countermeasures against verified non-governmental targets.

Risks and Constraints

Although the United States under Presidential Policy Directive 20 (PPD-20) has previously authorized government-backed cyber forces to conduct Defensive Cyber Effect Operations (DCEO) including, when necessary, active defense of the private sector, the problem has nonetheless persisted.[5] This may be partially attributed to U.S. private firms not wanting the U.S. government to have "the degree of access to and control over their networks and data needed" to execute DCEO.[6] Importantly, while we acknowledge there may be ongoing, unseen U.S. government active defense actions, if those actions are too covert or clandestine to be perceived, they are unlikely to affect an adversary's risk calculus. Separate active defense actions have also been executed in recent years by Western law enforcement agencies against malign actors. These law enforcement agencies have employed active defense, through technical takedowns that disrupt or seize cybercriminal infrastructure, including botnets, malware, and

command-and-control systems.[7] Despite these interventions by law enforcement, and likely the U.S. military, evidence suggests that U.S. private sector cyber exploitation has increased over time.[8]

Despite the urgency of the threat, the U.S. government has consistently constrained more assertive cyber responses by private cybersecurity firms. This is partially due to newness of the domain, which caused the government to approach it with caution. When compared to the number of adversarial cyberspace intrusions, this self-imposed restraint suggests that current U.S. cyber policy is weakening, rather than reinforcing, private-sector defenses. Indeed, private firms have long sought a change to this policy. Since at least 2013, American firms have sought government authorization to conduct limited hack-back activities to recover stolen data or to halt system exploitation.[9]

In fact, the debate about hacking back has been ongoing for at least the past twenty-five years, seemingly re-appearing almost every one to two years. Most of the arguments begin with why hacking back is a bad idea, and from there, find reasons to support their point of view. This has constrained policy discussion, thereby limiting U.S. imagination about what is possible, and ultimately setting back U.S. cyber defense. Overwhelmingly, hack-back policy discussions do not attempt to test their assumptions, and in even fewer instances does the conversation attempt to put forth a workable policy proposal to deal with cyberspace as it is, not as risk-averse U.S. policymakers continue to view it.

Undeniably, the first and best cybersecurity option is prevention, including building resiliency against cyber intrusion. This can include establishing incident response plans, data backup and recovery processes, and developing a culture of employee cybersecurity awareness.[10] In most cases, resilience is an appropriate policy for an organization, and while prevention remains essential, it is not sufficient in all cases. This can have severe consequences when U.S. private enterprises are targeted, resulting in harm to the U.S. economy and national defense.

Other hack-back discussions focus on a term called active defense. Legally, active defense is understood as consisting of "electronic countermeasures that attack an aggressive computer system, immobilizing that system and thus halting the cyber-attack." Demonstrating how long active defense has remained a neglected policy proposal, in a 2016 report from the Center for Cyber and Homeland Security, co-chaired by Admiral Dennis C. Blair, Michael Chertoff, Frank J. Cilluffo, and Nuala O'Connor, the first recommendation in the report explicitly suggests:

> *The Department of Justice (DOJ) should issue public guidance to the private sector with respect to active defense measures that it interprets to be allowable under current law, indicating that DOJ would not pursue criminal or civil action for such measures assuming that they are related to the security of a company's own information and systems.*[11]

Despite long-time advocacy for active defense from the U.S. private sector, the DOJ has yet to issue such formal guidance. We argue later that we should revisit and refine this 2016 proposal.

In private sector cybersecurity, active defense takes place across a spectrum, from the defender's own environment to producing effects in another's system. Active defense activities involve using visibility, analysis, and response capabilities inside networks and systems the defender legitimately owns or operates.[12] Active defense operations take place across four operational spaces: blue (IT systems and infrastructure under the jurisdiction of the state); green (IT systems and infrastructure leveraged in the malicious cyber operation/campaign that are under the jurisdiction of an allied or partner state); red (IT systems and infrastructure leveraged

in the malicious cyber operation/campaign that are under the jurisdiction of the originating state); and grey (IT systems and infrastructure that do not belong to any of the other spaces).[13] Except in the grey space, a state's repeated failure to comply with due diligence obligations regarding cyber exploitation emanating from their territory may give rise to international responsibility and justify proportionate active defense countermeasures.[14]

As active defense shifts from defensive actions (including "passive defenses" such as antivirus software) to offensive actions, activities outside one's own network carry more risk, requiring rigorous control [Figure 1].[15] "Passive" active defense measures taken inside one's own network can include, from least to most passive: honeypot/sandbox/tarpit/deception; intrusion reporting; passive intelligence gathering; and cyber hygiene/firewalls/scanning and monitoring.[16]

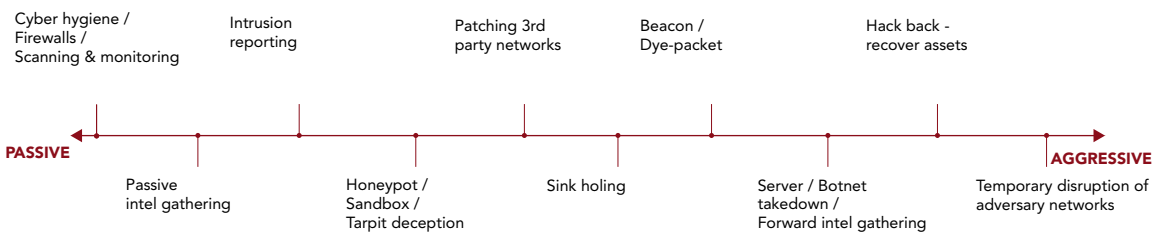
"Aggressive" active defense usually takes place outside of one's own network and can include from least to most aggressive: patching third party networks; sink holing; beacon/dye packet; server/botnet takedown, forward intelligence gathering; hack-backing to recover assets; temporary disruption of adversary networks; extended disruption of adversary networks; and hack-back to damage adversary assets.[17]

Observed Practice by Private Actors

U.S. laws prohibiting certain forms of active defense, such as hacking back, are difficult to reconcile with the observed behavior of both U.S. partners and malign actors. Estonia and Ukraine have already established pipelines for civilian cyber talent and private cyber organizations to support the defense of the country during hostilities. In 2010, Estonia stood up its Cyber Defense Unit, with Ukraine following in 2022 with the "IT Army of Ukraine." Importantly, neither Estonia nor Ukraine automatically disqualified someone from participating simply because they previously engaged in online criminal activity, including actions such as hacking back.[18] While both countries have a permissive approach to recruiting volunteer civilian cyber forces, it should be emphasized that all volunteers are vetted, and both states retain a degree of control over their volunteer cyber forces. Starting as far back as 2007, the Russian and Chinese governments also encouraged their own non-government "patriotic hackers," demonstrating an early willingness to blur the line between state and non-state cyber actors.[19]

In another example, China routinely employs ostensibly private cybersecurity companies and private individuals, or a hybrid mix, as seen in Salt Typhoon's use of Sichuan Juxinhe Network

Figure 1: Active Defense Spectrum



Source: figure adapted from Hoffman, Wyatt, and Ariel E. Levite. Private Sector Cyber Defense. Washington, DC: Carnegie Endowment for International Peace, 2017

Technology Co.[20] This group has targeted U.S. critical infrastructure, which is largely privately owned, without provoking a visible escalatory response. Similarly, in 2021, the Russian cybercriminal group DarkSide targeted Colonial Pipeline, deploying ransomware that disrupted fuel distribution along the U.S. East Coast.[21] Neither incident resulted in observable escalatory responses by the United States. These examples suggest that cyber intrusions, even when serious, do not automatically trigger uncontrollable escalation.

The following examples are part of a wider pattern involving China using non-governmental actors to target U.S. industry through cyberspace for intelligence gathering, further muddying the line between acceptable intelligence behavior and non-state criminal behavior. These campaigns were brought to light in a series of U.S. indictments from 2018 to 2025 where federal prosecutors documented a sustained pattern of China-linked cyber intrusions carried out through allegedly private Chinese companies and criminal actors. In December 2018, we learned Chinese actors operating via Huaying Haitai compromised managed service providers and dozens of global technology firms over more than a decade, enabling large-scale intellectual property theft while obscuring China's actions behind commercial actors.[22] In May 2019, a separate China-based non-governmental group was exposed and charged for intrusions culminating in the Anthem breach, which exposed data on nearly 79 million Americans.[23] There was also a July 2020 indictment of two Chinese nationals involved in a decade-long campaign exploiting vulnerabilities to steal vast quantities of sensitive data worldwide, sometimes for personal gain and sometimes in support of the Ministry of State Security (MSS).[24] That same year, indictments against Chinese actors tied to Chengdu 404 Network Technology revealed a system that blended intelligence collection with ransomware, crypto-mining, and fraud, all supported by private-sector infrastructure.[25]

Still further, in March 2025, prosecutors exposed i-Soon, a Shanghai-based hacker-for-hire firm that conducted intrusions, including operations targeting the U.S. government, and resold stolen data to numerous Chinese governmental agencies.[26] And in a July 2025 indictment, employees of Shanghai Powerock, allegedly acting under MSS direction, targeted U.S. COVID-19 researchers and participated in the HAFNIUM exploitation of Microsoft Exchange.[27] Collectively, these cases show a consistent model in which Chinese commercial entities, contractors, and criminals act against the U.S. private sector. Given the timeframe over which these actions have occurred, it does not appear China is working to constrain its private actors or fears serious consequences, especially criminal indictment.

It is not just nation-states that do not fear consequences. In an example of pushing back against a hack, in February of 2022, Lapsus$ claimed responsibility for a data breach of Nvidia. Nvidia claimed the group "took employee passwords and some Nvidia proprietary information from our systems and had begun leaking it online."[28] It is estimated that approximately 70 thousand Nvidia employee passwords were leaked. The attack briefly took part of Nvidia's operations offline.[29] Attention of the breach increased when a Lapsus$ group member alleged on Telegram that Nvidia had hacked them back. According to Lapsus$, and screen shots captured online, the ransomware group claimed that Nvidia hacked them back by infiltrating their network and encrypting files in their Virtual Machine (VM).[30] Nvidia did not engage publicly with those claims. Rather, the company confirmed the breach, acknowledged that employee credentials and proprietary information were being leaked, and stated that it had immediately hardened its network, brought in external incident-response experts, and notified law enforcement.[31] While there is no official information to corroborate the claim that Nvidia gained access into Lapsus$' VM, if true it appears Nvidia advanced

further along the active defense continuum than most private actors and appears to have faced no legal consequences.

In another case, GhostSec, also known as "Ghost Security," was formed in the wake of the 2015 attack on the Charlie Hebdo newspaper. GhostSec was believed to be composed largely of members of the decentralized "Anonymous" hacktivist group.[32] This group, including U.S. citizens, targeted ISIS-aligned extremist groups primarily on social media by identifying, publicizing, and targeting extremist groups' affiliated accounts. They also targeted standalone websites and used vulnerabilities to redirect, deface, or take down extremist affiliated websites. The group then split, forming two distinct groups: "Ghost Security Group," a de-anonymized group, seemingly aligned with United State government objectives, and "GhostSec" a group of original members working independently. Ghost Security Group is believed to have continued spying on extremist groups as opposed to hacking, while GhostSec was more aggressive, releasing a ransomware-as-a-service (RaaS) called "GhostLocker" in the fight against ISIS.[33] No group members have faced prosecution in the U.S. A hybrid model, one where there is a legal path for U.S. operators could likely have resulted in a different environment for both Ghostsec groups; one where they can disrupt violent extremist groups while also legally maintaining operations.

One final case is Muhstik, a ransomware attack targeting Linux-based Network Attached Storage devices from manufacturer QNAP.[34] Initially appearing in 2019, Muhstik encrypted the files on devices and then would generate a text file containing the information for payment to decrypt the files. In October of the same year, a user by the alias "battleck" posted to a public forum, claiming that he had "hacked back" the ransomware operators, and proceeded to dump every hash and decryption key publicly, allowing users to regain access to the files without paying the ransom.[35] "Battleck," who identified themself as Tobias Frömel admitted "i know it was not legal from me too but he used already hacked servers… and im not the bad guy here" [sic].[36] In effect, hacking back essentially severed the malicious actor's ability to extort users for ransom. This one user's actions to pursue the threat actors essentially nullified the potential profits and effectiveness of the Muhstik ransomware campaign on vulnerable QNAP devices. Frömel has not faced prosecution in Germany for his actions.

With these and other cases over the past twenty-five years, the U.S. prohibition against hacking back, a way to tactically impose costs in cyberspace, should be revisited. Yet, legacy U.S. cyber policymaking continues to cling to its preferred vision of how cyberspace should be organized, insisting that allowing private actors to respond in the domain will increase uncertainty and drive escalation. This claim is undermined by the fact that the U.S. public sector is routinely exploited in cyberspace by foreign private actors with little visible measurable response by the U.S. government. The logic is clearly flawed, revealing a failure within U.S. cyber policymaking that prioritizes outdated theoretical concerns over observed practice. Therefore, it is time to revisit some of our assumptions about the cyber domain.

This re-evaluation has occurred within the cyber strategy community where the debate shifted from the visions of "cyber 9/11" to a more measured and accurate view of the cyber domain.[37] By similarly adjusting its view of the cyber domain regarding private actors engaging in cyberspace, the U.S. government can create a cyber strategy that better reflects the behavior in the domain. Revisiting past prohibitions on hack-backs, which have been a simple "don't do it or else" policy, and comparing real-world outcomes with experts' predictions, and then cautiously testing new assumptions to redefine acceptable boundaries in

cyberspace, would appear a policy worth pursuing. While the U.S. government continues to operate under untested assumptions, its adversaries are actively employing its private cyber actors against the United States' private sector.

Concerns and Assumptions

Concerns about hacking back have long centered on issues like operator security, attribution, escalation, and loss of control. Retaliatory cyber activity could expose cybersecurity professionals to identification, detention, coercion, or violence. While this is a valid concern, it also raises questions about whether these risks are widespread or confined to a limited number of isolated cases. Much of the other existing debate emphasizes why hacking back should not be legalized, highlighting unreliable attribution, mistargeting, escalation dynamics, and the potential compromise of ongoing operations.

Attribution concerns are particularly acute. Determining whether an intrusion originated from an adversary system or from infrastructure that has itself been compromised introduces uncertainty, and a response risks harming an innocent third party. These risks underscore why it would be irresponsible for unvetted or uncontrolled operators to respond independently. At the same time, these concerns argue for caution rather than absolute prohibition. Many cybersecurity professionals who would be involved in such activities would likely come from the national security community and are accustomed to operating under strict rules of engagement, including operating with incomplete information and minimizing collateral effects.[38] However, concerns about uncertainty have hardened into a near-commandment that private cybersecurity actors must never aggressively respond to malign activity, or they will charged under federal law. While it is difficult to determine how many CFAA cases are prosecuted each year, one source documented 165 such cases in 2017.[39] These cases involved a wide range of CFAA violations, almost all of which had nothing to do with active defense as the concept is applied in the article.

A related assumption is that private companies lack the ability to reliably identify malicious actors exploiting their systems. While this may be true for some smaller firms, it does not hold uniformly. Large, well-resourced cybersecurity firms routinely track persistent threat actors across multiple campaigns and possess advanced technical capabilities to identify the actors.[40] In some cases, private counteractions illuminate adversarial infrastructure and sponsorship, reducing uncertainty and validating national-level cyber forces response to the exploitation.

In addition, critics often assume that any private response must mirror state-level cyber operations since it could provoke a state counterreaction. This assumption treats escalation as automatic, overlooking the fact that private cybersecurity firms already engage in actions, such as takedown requests and legal seizure of infrastructure, that impose costs without triggering escalation.[41] Consequently, more limited actions, focused on verified non-governmental infrastructure, do not require equivalence with nation-state capabilities to have an effect.

Allowing private hacking back also raises concerns over coordination and control since private actors have no visibility into ongoing government operations. The argument is that in allowing hacking back, private cybersecurity actors could unintentionally delete evidence, unknowingly interfere with classified activity, or disrupt an active investigation.[42] Thankfully, a relationship has been built over time between law enforcement (and the federal government) and with select cybersecurity firms which could partially mitigate this concern. An additional issue with allowing hacking back is that private forces could not be controlled.[43] This assumption, that the government could not control private-sector action, is undermined by case of the

2020 Trickbot takedown, which was a form of active defense in coordination with the private sector.

In this case, legal counsel from Microsoft and USCYBERCOM leveraged trademark law to act against the target. The Trickbot malware operation was designed to steal banking credentials and Microsoft argued that Trickbot's operators were misusing Microsoft trademarks by distributing malware that appeared to incorporate Microsoft software.[44] Timing their move while Microsoft's legal-tech action was underway, USCYBERCOM ran an operation that injected false commands into the Trickbot network, severing parts of its control infrastructure. Backed by the courts, Microsoft disabled IP addresses used by Trickbot's command-and-control servers, rendering content on those servers unreachable, blocking the botnet from leasing new servers, and coordinated with ISPs and telecoms to legally enforce those disruptions.[45] Clearly, there is a need for more innovative interventions like the Trickbot takedown, demonstrating a greater need to open-up the policy discussion around active defense.

Legal Mechanisms and Feasibility

Within this context, there is broad recognition that existing legal frameworks constrain private cyber activity. Recent legislative efforts, including the Active Cyber Defense Certainty Act (2019), reflect attempts to provide cybersecurity professionals with greater authority to impose costs.[46] Other policy proposals have argued that prevailing interpretations of the CFAA have sidelined private U.S. cybersecurity capability, even as the government has long relied on private contractors in other domains to impose costs.[47]

Some hack-back supporters contend that the CFAA's prohibitions are so expansive that they risk being unconstitutionally vague, allowing courts to apply the rule of lenity.[48] Others point to common-law traditions permitting limited self-help to prevent theft, or to statutory language stating that the CFAA does not prohibit lawfully authorized investigative or protective activities by law enforcement or intelligence agencies.[49] To hack-back advocates, this language has been interpreted as leaving room for federal agencies to authorize certain private cybersecurity actions. Additional hack-back proposals suggest that acceptable use policies or the doctrine of necessity could justify limited countermeasures under specific circumstances.[50] For instance, an acceptable use policy (AUP) could be construed such that when an external actor connects to Company A's network, that actor implicitly accepts the company's AUP. If this premise is accepted, the company could argue that it has permission to observe or interact with the connection in ways that might otherwise be restricted.[51]

Yet still, there are other less explored avenues to bring U.S. private cyber capabilities off the sideline while still providing for oversight and accountability. Some supporters of hacking back argue federal statutes may be interpreted as permitting private action when conducted with government authorization. For example, 18 U.S.C. § 1030(f) provides that the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency."[52] To some, this provision could be read to allow federal agencies to authorize private cybersecurity firms to carry out certain countermeasures on the government's behalf. Similarly, Section 104 of the Cybersecurity Information Sharing Act of 2015 (CISA) authorizes private entities, "for cybersecurity purposes," to monitor or operate a defensive measure on their own information systems, or if they have written authorization, on the systems of another non-federal entity.[53] In essence, the act does not explicitly prohibit actual hack-back.

Despite these novel policy and legal arguments, there is broad agreement that creating new interpretations of or exemptions to the CFAA would require protracted political and legal battles that the

United States cannot afford. Rather than attempting to rewrite statutory meaning, a more feasible approach would be formal authorization through long-overdue Department of Justice guidance permitting limited hack-back actions. Such guidance would operate within existing law, constrain scope and actors, and specifically address long-standing concerns about uncertainty, escalation, and control by placing private activity within a transparent and accountable legal framework.

Loosening Self-Imposed Restraints

Although in this article we have at times referenced hack-back operations in the context of other countries' national defense, we do not argue that private cybersecurity firms be permitted to operate in coordination with the intelligence community or the military, nor to target foreign government or military systems. Rather, we advocate for incremental adjustments authorized through formal DOJ guidance to authorize limited hacking back to mitigate an ongoing problem afflicting U.S. private industry. If given legal authorization by the DOJ, this guidance would not be subject to subsequent liability under the CFAA so long as verified private cybersecurity firms did not exceed authorized actions.[54] Under these conditions, permitting selected U.S. private cybersecurity firms to have limited hack-back effects would not be destabilizing but rather increase order through controlled responses to foreign private actions. Under our proposal, if a targeted actor responds aggressively or the situation escalates, the U.S. private cybersecurity firm would disengage and notify the U.S. government, allowing appropriate federal operators to assume responsibility.

As a starting point, DOJ guidance authorizing more aggressive active defense might sound like the following:

This DOJ guidance establishes limited private counter measures to protect U.S. private networks by combining active defensive measures with timely information sharing and cooperative action with federal law enforcement. It does not permit the most aggressive active defense measures or actions taken by unvetted, independent actors. With this directive, the DOJ reaffirms that private sector active defensive measures must comply with federal criminal law, except when given specific authorization to access systems beyond one's own network. Any contemplated active defense actions that go beyond activities on one's own network must be evaluated with counsel and in consultation with federal partners to determine appropriate legal authorization. Before responding to any network exploitation, authorized U.S. private sector cybersecurity firms must engage early with federal law enforcement to ensure actions are lawful and coordinated with ongoing investigations and operations. Private actors must avoid unilateral operations that any reasonable person would deem risks unacceptable collateral damage or escalation.

The least aggressive form of hacking back we advocate for are actions to recover assets, which could take the form of erasing the memory of a computer that has penetrated a victim's network or to extract data from the victim's systems. At its most aggressive, we advocate for temporary disruption of adversary networks in the form of a Distributed Denial of Service (DDOS) attack (the metaphorical "stun"). The DDOS attack would serve to overwhelm the attacker's network with traffic from external sources, thereby blocking the attacker's ability to access their own systems thus stopping the on-going exploitation. Both measured actions would demonstrate to the adversary there are costs for their activities, and that the U.S. has chosen to respond within the confines of active defense rather than escalate and exacerbate the situation. Notably, our proposal does not recommend the most aggressive forms of hacking back but rather incremental adjustments to test how the environment responds.

In the United States, some have argued that bringing hack-back out of the shadows would reduce the risk of uncoordinated actions by ensuring that activity aligns with a defined strategy.[55] Thus, by authorizing hack-back, select private firms would increase transparency and control over actions that already occur cyberspace. Additionally, our proposal calls for employing private cyber firms that have been properly vetted and authorized to more aggressively actively defend networks. This is in sharp contrast to employing individual private actors that have untested capabilities and operate independent of a shared objective. In the same way private security firms are prohibited from deploying armed guards without background checks and appropriate firearm training, private cybersecurity companies with active defense capabilities would be subject to comparable vetting and certification standards.[56] Private firms would be able to choose from a list of approved hack-back vendors, who could credibly threaten a response to a foreign private cyberspace exploitation.[57]

The more aggressive active defense actions would extend existing private defensive operations, as opposed to creating an entirely new category of response. Today's U.S. cybersecurity companies can extend the reach of their activities.[58] They already possess some of the most advanced technical cybersecurity capabilities, and the scope of their reach rivals some governments. For example, Microsoft's processes the order of 100 trillion security signals per day, while applying automatic malware blocking and identity-risk detections.[59] Likewise, Google Cloud's Mandiant M-Trend's report is informed by 450,000 hours of Mandiant Consulting Investigations, and Verizon's Data Breach Investigations Report is based on an analysis of over 22,000 real-world security incidents.[60] These and other private cybersecurity firms already operate with technical maturity at operational scale, meaning it is highly likely they have the capability to engage in proportional active defense actions.

By permitting techniques to pursue malign actors, while introducing oversight to prohibit destructive actions, private cybersecurity could extend their operations beyond the network in a legally defensible way. While oversight can also create the risk of operational delay, this tradeoff is acceptable if it enables timely, proportionate disruption of ongoing threats while preserving accountability, control, and alignment with broader U.S. strategy. The establishment of a federally "verified" status, and the implementation of rigorous internal controls mitigates some of the concern surrounding private active defense, such as misattribution, escalation, or even collateral damage. Under a defined scope and safeguards, private entities would operate with standard "rules of engagement" in cyberspace, requiring mandatory coordination with authorities, while ensuring that active defense actions are proportional, fair, and aligned.

Creative responses to cyber exploitation have been available the entire time. What has been needed is the opening-up of a policy discussion. The duration and seriousness of this issue emphasize the need for the United States government to consider new and different ways of defending its private sector. The U.S. has allies and partners, and adversaries, who demonstrate different ways of thinking about the cyberspace domain, and whom themselves have crossed the private sector-government divide without catastrophic consequences. The U.S. should learn, and adapt its cyber defenses, based on others' experiences.

Conclusion

A state's cybersecurity requires taking actions within the parameters of its domestic law. When a country imposes restraints based upon speculative concerns, its national (cyber)security is diminished. This helps explain why debates over

hacking back have remained stalled. In this article, we revealed that there are existing private entities that operate within the U.S. to hack-back, and when hacking back has historically occurred, there has not been uncontrolled escalation, and the U.S. legal system has largely ignored the private actor hack-back.

Rather than continue to watch the slow cyber-based exploitation of the U.S. private sector, policymakers should adapt to the environment and create change to alter malign behavior. These challenges to policymakers help clarify how their beliefs about cyberspace work in practice. Rather than challenge assumptions, the U.S. cyber policy community has entirely evaded discussion around a fully resourced cybersecurity proposal. Instead of testing the boundaries of policy, the U.S. government has largely stood by as its private industry has endured massive exploitation by foreign private cyberspace actors. All too often policymakers have offered explanations for what could not be done to protect industry rather than proposals for what could. Institutional cyber policymakers have grown complacent, forgetting a core purpose of U.S. cybersecurity policy--protecting American economic interests. The result has been cyber policies that lag the threat environment as U.S. private industry suffers.

To distinguish the policy recommendation in this paper and move beyond past debates narrowly focused on the CFAA, we offered an updated policy framework, through formal DOJ guidance, that could work with the confines of current U.S. law. The least aggressive form of hacking back we advocate for are actions to recover assets which could take the form of erasing the memory of a computer that has penetrated a victim's network or to extract data from the victim's systems. At its most aggressive, we advocate for temporary disruption of adversary networks in the form of a DDOS attack. Both measured actions would demonstrate to the malign private actors there are costs for their actions, and that the U.S. has chosen to defensively respond within the confines of active defense rather than escalate the situation. Notably, our proposal does not even recommend the most aggressive form of hacking back but instead advocates for testing how the environment responds to new controlled, incremental actions.

Ultimately, this article sought to reframe the debate, enabling the U.S. government to draw on a previously underutilized capability, limited private-sector hack-back. This is a significant step since it would free U.S. cyber policy from self-imposed constraints that do not bind its competitors. In practice, it would expand the capacity to protect U.S. private property, while allowing national-level cyber forces to focus on higher-priority threats. Absent such adaptation, the United States will continue to concede the initiative in cyberspace not because it lacks capability to protect its private sector, but because it chose to defend itself with one hand.

Endnotes

[1] Hoffman, Wyatt, and Ariel E. Levite. *Private Sector Cyber Defense*. Washington, DC: Carnegie Endowment for International Peace, 2017. https://carnegie-production-assets.s3.amazonaws.com/static/files/Cyber_Defense_INT_final_full.pdf.

[2] Broeders, Dennis. "Private Active Cyber Defense and (International) Cyber Security—Pushing the Line?" *Journal of Cybersecurity* 7, no. 1 (March 30, 2021). https://academic.oup.com/cybersecurity/article/7/1/tyab010/6199903.

[3] Kello, Lucas. "Private Sector Active Defense: An Adequate Response to the Sovereignty Gap?" In *The Virtual Weapon and International Order*, 229–246. New Haven, CT: Yale University Press, 2017. https://doi.org/10.12987/9780300226294-012.

[4] Sella, Adam. "U.S. Weighs Expanding Private Companies' Role in Cyberwarfare." *New York Times*, January 14, 2026. https://www.nytimes.com/2026/01/14/us/politics/us-cyberwarfare-private-companies.html

[5] PPD-20 is a 2012 Obama-era presidential directive that established U.S. policy and interagency procedures for the planning, approval, and oversight of offensive and defensive cyber operations.; Flowers, Angelyn, and Sherali Zeadally. "US Policy on Active Cyber Defense." *Journal of Homeland Security and Emergency Management* (June 19, 2014). https://www.degruyterbrill.com/document/doi/10.1515/jhsem-2014-0021/html.

[6] Hoffman, Wyatt, and Ariel E. Levite. *Private Sector Cyber Defense*. Washington, DC: Carnegie Endowment for International Peace, 2017. https://carnegie-production-assets.s3.amazonaws.com/static/files/Cyber_Defense_INT_final_full.pdf.

[7] Wilde, Gavin, and Emma Landi. "Exploring Law Enforcement Hacking as a Tool against Transnational Cyber Crime." *Carnegie Endowment for International Peace*, April 23, 2024. https://carnegieendowment.org/research/2024/04/exploring-law-enforcement-hacking-as-a-tool-against-transnational-cyber-crime.

[8] Total Assure. "Cyber Attack Statistics by Year: 2020–2025 Data Reveals Unprecedented Growth in Global Threats." *Total Assure Blog*, October 21, 2025. https://www.totalassure.com/blog/cyber-attack-statistics-by-year-2020-2025.

[9] Commission on the Theft of American Intellectual Property. *The IP Commission Report*. United States, 2013. Web Archive. https://www.loc.gov/item/lcwaN0009018/.

[10] Parenty, Thomas J., and Jack J. Domet. A Leader's Guide to Cybersecurity: *Why Boards Need to Lead—and How to Do It*. Boston: Harvard Business Review Press, 2019. https://store.hbr.org/product/a-leader-s-guide-to-cybersecurity-why-boards-need-to-lead-and-how-to-do-it/10289.

[11] Lainhart, John. "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats." *IBM Center for the Business of Government*, November 29, 2016. https://www.businessofgovernment.org/blog/gray-zone-private-sector-and-active-defense-against-cyber-threats.

[12] Kello, Lucas. "Private Sector Active Defense: An Adequate Response to the Sovereignty Gap?" In *The Virtual Weapon and International Order*, 229–246. New Haven, CT: Yale University Press, 2017.

[13] Herpig, Sven. "Active Cyber Defense—Toward Operational Norms." *Transatlantic Cyber Forum*, November 2023. https://www.interface-eu.org/publications/downloadPdf/active-cyber-defense-toward-operational-norms.

[14] Shackelford, Scott J., Scott Russell, and Andreas Kuehn. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors." *Chicago Journal of International Law* (2016). https://cjil.uchicago.edu/print-archive/unpacking-international-law-cybersecurity-due-diligence-lessons-public-and-private.

[15] Dine, Alexandra Van. "When Is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures under the Budapest Convention." *Chicago Journal of International Law* (2020). https://cjil.uchicago.edu/print-archive/when-cyber-defense-crime-evaluating-active-cyber-defense-measures-under-budapest.

[16] A honeypot is a decoy system designed to attract and monitor cyber attackers, allowing defenders to study intrusion methods and divert threats away from real assets. A sandbox is an isolated computing environment used to safely execute and analyze suspicious code or files without risking damage to the host system or network. A tarpit is a network defense mechanism that deliberately slows down incoming connections, wasting an attacker's time and resources to discourage automated scanning and exploitation. Deception is a defensive strategy that uses false information, decoy assets, or misleading network configurations to confuse attackers and detect unauthorized activity.

[17] Hoffman, Wyatt, and Ariel E. Levite. *Private Sector Cyber Defense*. Washington, DC: Carnegie Endowment for International Peace, 2017. https://carnegie-production-assets.s3.amazonaws.com/static/files/Cyber_Defense_INT_final_full.pdf. Patching third-party networks refers to the practice of applying security updates or fixes to networks or systems not owned by the defender, typically to close vulnerabilities being actively exploited by attackers. Sink holing is a technique that redirects malicious network traffic, such as communications between malware and its command server to a controlled server, effectively neutralizing the threat and enabling analysis. A beacon or dye packet is a trace-back technology that embeds hidden digital markers in data, enabling defenders to track stolen information and establish attribution when it is accessed or exfiltrated by an adversary. A server or botnet takedown is the coordinated seizure or disruption of malicious infrastructure to halt ongoing cyberattacks.

[18] Done, William D. "The Information Technology Army of Ukraine and Cyber Warfare Doctrine." *Journal of Strategic Security* (2023). https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1005&context=jss. Svantesson, Dan Jerker B. "Regulating a 'Cyber Militia': Some Lessons from Ukraine, and Thoughts about the Future." *Scandinavian Journal of Military Studies* (July 11, 2023). https://sjms.nu/articles/10.31374/sjms.195.

[19] Grzegorzewski, Mark, and Christopher Marsh. "A Strategic Cyberspace Overview: Russia and China" In *Great Power Cyber Competition*, pp. 6-24. Routledge, 2024.

[20] Cybersecurity and Infrastructure Security Agency (CISA). "Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide to Feed Global Espionage System." September 3, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

[21] Freed, Anthony M. "Inside the DarkSide Ransomware Attack on Colonial Pipeline." *Cybereason Blog*. Accessed January 12, 2026. https://www.cybereason.com/blog/inside-the-darkside-ransomware-attack-on-colonial-pipeline.

[22] United States Department of Justice. "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." December 20, 2018. https://www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[23] United States Department of Justice. "Seven International Cyber Defendants, Including 'APT41' Actors, Charged in Connection with Computer Intrusion Campaigns against More Than 100 Victims Globally." September 16, 2020. https://www.justice.gov/archives/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

[24] United States Department of Justice. "Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc." May 9, 2019. https://www.justice.gov/archives/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including.

[25] United States Department of Justice. "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research." July 21, 2020. https://www.justice.gov/archives/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

[26] United States Department of Justice, United States Attorney's Office for the District of Columbia. "Chinese Nationals with Ties to the PRC Government and 'APT27' Charged in a Computer Hacking Campaign for Profit." March 5, 2025. https://www.justice.gov/usao-dc/pr/chinese-nationals-ties-prc-government-and-apt27-charged-computer-hacking-campaign-profit.

[27] United States Department of Justice, Office of Public Affairs. "Justice Department Announces Arrest of Prolific Chinese State-Sponsored Contract Hacker." July 8, 2025. https://www.justice.gov/opa/pr/justice-department-announces-arrest-prolific-chinese-state-sponsored-contract-hacker.

[28] Nvidia Support. "Security Notice: NVIDIA Response to Security Incident - March 2022." March 8, 2022. https://nvidia.custhelp.com/app/answers/detail/a_id/5333/~/security-notice%3A-nvidia-response-to-security-incident---march-2022.

[29] Arntz, Pieter. "Nvidia, the Ransomware Breach with Some Plot Twists." *ThreatDown by Malwarebytes*, March 3, 2022. https://www.threatdown.com/blog/nvidia-the-ransomware-breach-with-some-plot-twists/.

[30] Ghosh, Soumik. "How Lapsus$ Data Leak May Affect Nvidia and Its Customers." *Bank Information Security*, March 1, 2022. https://www.bankinfosecurity.com/how-lapsus-data-leak-may-affect-nvidia-its-customers-a-18636.

[31] Newman, Lily Hay. "The Lapsus$ Hacking Group Is Off to a Chaotic Start." *Wired*, March 15, 2022. https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/.
[32] Tynes, Robert. "When GhostSec Goes Hunting." *LIMN*, University of California, Los Angeles, 2017. https://escholarship.org/content/qt0fk3m0g7/qt0fk3m0g7_noSplash_05cdccc9f591e5c9389d9c5cca0b47e9.pdf.
[33] Wendling, Mike. "Ghost Security Group: 'Spying' on Islamic State Instead of Hacking Them." *BBC News*, November 23, 2015. https://www.bbc.com/news/blogs-trending-34879990.
[34] QNAP Systems, Inc. "Security Advisory for Muhstik Ransomware." October 4, 2019. https://www.qnap.com/en-us/security-advisory/nas-201910-02.
[35] Stahie, Silviu. "Developer Hacks Back Against Ransomware Attackers and Steals Decryption Keys." *Bitdefender*. October 9, 2019. https://www.bitdefender.com/en-us/blog/hotforsecurity/developer-hacks-back-against-ransomware-attackers-and-steals-decryption-keys.
[36] Frömel, Tobias ("battleck"). "Muhstik (QNAP NAS) Ransomware (.Muhstik) Support Topic." *BleepingComputer Forums*, October 7, 2019. https://www.bleepingcomputer.com/forums/t/705604/muhstik-qnap-nas-ransomware-muhstik-support-topic/page-9#entry4882035.
[37] Skingsley, Juliet. "Offensive Cyber Operations." *Chatham House*, September 19, 2023. https://www.chathamhouse.org/2023/09/offensive-cyber-operations/02-perceptions-utility.
[38] Fay, Joe. "Why so many military veterans move into cybersecurity." *BBC News*, May 22, 2025. https://www.bbc.com/news/articles/ce3vgjzwl04o.
[39] Martens, Philippe. "Self-Defence in Cyberspace: Hacking Back the Hacker." Tilburg University, January 2021. https://arno.uvt.nl/show.cgi?fid=155524.
[40] Cyber Advisory. "Top 10 Best Cyber Threat Intelligence Companies in 2026." *Cyber Security News*, January 1, 2026. https://cybersecuritynews.com/best-cyber-threat-intelligence-companies-2/.
[41] Broeders, Dennis. "Private Active Cyber Defense and (International) Cyber Security—Pushing the Line?" *Journal of Cybersecurity* 7, no. 1 (March 30, 2021).
[42] Cyber Tech Accord. "No Hacking Back: Vigilante Justice Vs. Good Security Online." *Cyber Tech Accord*, November 19, 2020. https://cybertechaccord.org/uploads/prod/2020/11/hack-back-update-131120-pages.pdf.
[43] Couzigou, Irene. "Hacking-back by private companies and the rule of law." *Heidelberg Journal of International Law* (2020).
[44] Microsoft Threat Intelligence. "Trickbot disrupted." *Microsoft Security*, October 12, 2020. www.microsoft.com/en-us/security/blog/2020/10/12/trickbot-disrupted/.
[45] Vavra, Shannon. "Cyber Command, Microsoft take action against TrickBot botnet before Election Day." Cyberscoop, October 12, 2020. https://cyberscoop.com/trickbot-takedown-cyber-command-microsoft.
[46] Chesney, Robert. "Hackback Is Back: Assessing the Active Cyber Defense Certainty Act." *Lawfare*, June 24, 2019. https://www.lawfaremedia.org/article/hack-back-back-assessing-active-cyber-defense-certainty-act.
[47] Parker, Sam. "Shot in the Dark: Can Private Sector "Hackbacks" Work?" *Center on National Security Georgetown Law*, December 16, 2020. https://nationalsecurity.law.georgetown.edu/journal/2022/12/16/shot-in-the-dark-can-private-sector-hackbacks-work/.
[48] Rabkin, Jeremy and Ariel Rabkin. "Hacking Back Without Cracking Up." *Hoover Institute* (2016). https://www.hoover.org/sites/default/files/research/docs/rabkin_webreadypdf.pdf.
[49] Baker, Stewart, Orin Kerr, and Eugen Volokh. "The Hackback Debate." *Steptoe*, November 2, 2012. https://www.steptoe.com/en/news-publications/cyberblog/the-hackback-debate.html.
[50] Lachow, Irving. "Active Cyber Defense A Framework for Policymakers." *Center for a New American Security* (2013). https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers.
[51] Lachow, Irving. "Active Cyber Defense A Framework for Policymakers." *Center for a New American Security* (2013). https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers.
[52] Congressional Research Service. "Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes." May 16, 2023. https://www.congress.gov/crs-product/R47557.
[53] Carlin, John. "So You Want to Hack-back: Here's What You Should Know." *Aspen Digital*, October 9, 2025. https://www.aspendigital.org/blog/so-you-want-to-hack-back/.
[54] Rabkin, Jeremy and Ariel Rabkin. "Hacking Back Without Cracking Up." *Hoover Institute* (2016). https://www.hoover.org/sites/default/files/research/docs/rabkin_webreadypdf.pdf.
[55] Waterman, Sean. "Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts." *Newsweek*, February 21, 2023. https://www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970.
[56] Gates, Megan. "Training Builds Frameworks of Support for Armed Security Personnel." *Security* Management, June 21, 2025. https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2025/june/training-armed-security-personnel/.

[57] Rabkin, Jeremy and Ariel Rabkin. "Hacking Back Without Cracking Up." *Hoover Institute* (2016). https://www.hoover.org/sites/default/files/research/docs/rabkin_webreadypdf.pdf.
[58] Starks, Tim. "Google previews cyber 'disruption unit' as U.S. government, industry weigh going heavier on offense." *Cyberscoop*, August 27, 2025. https://cyberscoop.com/google-cybersecurity-disruption-unit-active-defense-hack-back/.
[59] Microsoft. "Microsoft Digital Defense Report 2025." https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1.
[60] Verizon Business. "Report 2025 Data Breach Investigations." https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf; Google Cloud. "M-Trends 2025: Data, Insights, and Recommendations From the Frontlines." *Threat* Intelligence, April 23, 2025. https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025.

Preparing Populations for Hybrid Attacks Against Critical Infrastructure[1]

By Dr. Heather S. Gregg

Introduction

On May 7, 2021, specialists monitoring the Colonial Pipeline, a Houston-based facility that distributes gasoline across the southeastern United States, detected a security breach in its Information Technology system. The company quickly shut down its computer system and the distribution of gasoline through its 5,500 miles of pipelines. A hacking group calling itself "DarkSide" demanded 75 Bitcoin, approximately 4.4 million U.S. Dollars at the time, for the decryption key to the malware that had infected the system.[2]

As news spread of the ransomware attack and Colonial Pipeline's decision to shut down the pipeline, panic began to set in across several states on the East Coast. Long lines formed at gas stations in Florida, Georgia, Alabama, Virginia and the Carolinas and people began to hoard gas. Online rumors circulated that some even tried to put gasoline in plastic shopping bags, prompting a national call for consumers to not engage in this activity. State authorities attempted to calm populations by assuring them that there was enough gas if people did not panic and hoard fuel. This message, however, did little to change behavior.[3] On May 9th, Colonial Pipeline paid the ransom for the decryption key and resumed pumping gasoline throughout its system. President Joseph R. Biden, Jr., addressed the nation on May 14 and implored, "Don't panic…I know seeing lines at the pumps or gas stations with no gas can be extremely stressful, but this is a temporary situation. Do not get more gas than you need in the next few days."[4] Eventually consumer behavior returned to

Dr. Heather S. Gregg is a research fellow at the Future Security Initiative at Arizona State University. Her academic focus is on irregular warfare, hybrid threats, terrorism and counterterrorism, causes of extremism, and leveraging culture in population centric conflicts, including resiliency and repairing communities and national unity in the wake of war and political instability. She has held several academic positions in the U.S. Department of Defense, including professor of Irregular Warfare/Hybrid Threats at the George C. Marshall European Center for Security Studies (2023-2024), professor of military strategy at the U.S. Army War College (2019-2022), and associate professor at the Naval Postgraduate School in Monterey, California, where she worked primarily with Special Operations Forces (2006-2019). She is the author of "Hybrid Threats and Strategic Competition" (Connections 2024); Religious Terrorism (Cambridge University Press, 2020); and Building the Nation: Missed Opportunities in Iraq and Afghanistan (University of Nebraska 2018).

normal as it became clear that the crisis had ended. An FBI-led investigation suggested that *DarkSide* had connections to Russia, but these ties could not be definitively proven.[5]

The attack on the Colonial Pipeline may have been more than just a profit-seeking group's desire to extort money through ransomware. It may actually have been a hybrid attack from a state working through "proxies"—individuals and groups that provide a degree of deniability to the state and may or may not be working directly with the state—to execute illegal actions with the goal of causing mass panic, undermining the government's credibility, and weakening its ability to project power both internally and internationally. Hybrid attacks against critical infrastructure (CI), like the Colonial Pipeline, are especially challenging for governments because they are difficult to prevent, attribute to an actor, and not only affect a population's access to critical goods and services but also diminish their trust in the government's ability to protect CI and provide these goods and services when attacks occur. Furthermore, when executed effectively, the population's response to hybrid threats becomes part of the attack itself. Populations panic, amplifying the attack, and force governments to devote time and resources to restore order, as was the case with the Colonial Pipeline incident. Preparing populations for disruptions to goods and services caused by hybrid attacks against CI is necessary for explaining the nature of hybrid threats, reducing panic, and helping to undermine the adversary's plan.

To make these points, the article proceeds as follows: The first section provides a brief overview terminology, specifically irregular warfare, hybrid threats, and hybrid attacks. It also offers a working definition of Critical Infrastructure, outlines why hybrid attacks against CI are a particularly effective weapon and difficult to prevent, and why countries need to foster societal resilience to prepare for and resist these attacks. The second section investigates Europe's experience defending against and responding to hybrid attacks against CI, including measures taken by the European Union and NATO to prepare for hybrid attacks to CI. The third section looks specifically at how Sweden, the United Kingdom and Romania have defended against hybrid attacks to CI and prepared their populations for disruptions to goods and services caused by these attacks. And the final section offers key takeaways from the European experience.

Irregular Warfare and Hybrid Attacks on Critical Infrastructure

One of the first challenges in preparing populations for hybrid attacks against CI is a lack of consensus on what to call the range of hostile activities that adversaries use to undermine trust between populations and their governments, or if these activities even rise to the level of warfare.

The United States uses the term **Irregular Warfare (IW)** to describe a range of hostile activities that fall outside traditional state-on-state warfare between uniformed, organized militaries. U.S. Joint Doctrine 1 Vol. 1, "Joint Warfighting" (2023) defines IW as "a form of warfare where state and non-state actors' campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities, either as the primary approach or in concert with conventional warfare."[6]

The concept of IW, critically, includes a range of hostile activities that are "indirect. The U.S. Department of War's (DOW) Irregular Warfare Center (IWC), for example, draws on U.S. doctrine and similar guidance to include activities such as terrorism, cyberwarfare, sabotage, insurgency, guerilla warfare, and proxy warfare, as examples of indirect activities as examples of IW.[7] States and nonstate actors use these activities to weaken their adversary without direct military confrontation, and often states work through nonstate actors, including proxies, to achieve these effects.

The IWC identifies **hybrid threats** as a specific subset of activities within IW. One of the most cited definitions of hybrid threats comes from the Helsinki Hybrid Center of Excellence (Hybrid COE). It describes hybrid threats as a "concept" that,

> *…refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.*[8]

Hybrid COE's concept stresses that hybrid threats aim to "deliberately target democratic states' and institutions' vulnerabilities" with the overall goal of undermining a country's political system, that they are coordinated and synchronized to have this effect. Hybrid threats, in other words, could be just about anything, so long as they have the wider effect of aiming to undermine the political system and prevent states from projecting power inward and internationally. Mark Galeotti famously calls this "the weaponization of everything."[9] Protecting CI from hybrid threats has several challenges. First, there is no consensus on what sectors constitute CI. One **definition describes CI** as "the physical and cyber systems and assets that are so vital to a country that their incapacity or destruction would have a debilitating impact on a nation's physical or economic security or public health and safety."[10] Given this definition, countries will have their own lists of what comprises CI based on geography, infrastructure, population, vulnerabilities and needs.

Most states recognize four "critical lifeline" sectors of energy, water, transportation and communications infrastructure as CI.[11] However, a fifth category, financial infrastructure, should also be included when preparing populations for and recovering from hybrid attacks on CI. Disruptions to the financial sector, from Distributed Denial of Service (DDoS) attacks, ransomware, GPS jamming and other hybrid attacks, present a particular vulnerability that could be exploited by adversaries and cause mass panic in populations. This is especially true if hybrid attacks prevent people from having access to their money, including being able to pay for items digitally and to withdraw cash.[12]

Second, most countries' CI includes a mixture of government and privately owned companies and enterprises, making protecting CI challenging. These partnerships require delineation of who is responsible for protecting services, including both formal laws and authorities as well as collaboration through less formal channels before attacks occur, and plans and procedures for what to do once attacks on privately provided CI do occur.

Third, CI is almost always interconnected; an attack on one sector most likely will affect other sectors as well, causing a cascading crisis. For example, electricity is required to run virtually every other CI sector in any given country and, while generators and other temporary sources of power can provide electricity in times of crisis, major disruptions to a country's supply of electricity will have cascading effects across CI sectors.[13]

Fourth, failures of CI in one country can also affect CI in other countries. For example, in 2017, the Danish shipping company Maersk was hit with a cyberattack that took down their computer system, paralyzing their operations for days, shutting down ports, and affecting shipping around the world. The malware, called "NoTPetya," was attributed to a hacking group with ties to the Russian military that intended to hit Ukrainian CI but infected and

disrupted the Danish shipping company's computer system as well.[14]

Fifth, predicting hybrid attacks against CI is difficult if not impossible to do. Other threats to CI, like natural disasters, can often be predicted based on seasons (like hurricanes) or locations (such as earthquakes), and regions that are prone to these activities can take preparatory and defensive measures to secure CI. Hybrid attacks against CI, however, can occur anywhere at any time making prevention very difficult if not impossible.

Given the intentionality of these attacks and the key role that the population's response plays, hybrid attacks against CI are more like terrorism than natural disasters. Terrorist acts bear similarity to hybrid attacks on CI because they aim to instill fear in populations and cause them to panic. However, groups perpetrating terrorist attacks typically claim responsibility for their actions as a form of publicity and recruitment. In hybrid attacks, states will aim to conceal their involvement through proxies and other means to prevent legal actions, counterattacks, or escalation.[15] Preparing populations to withstand and recover from hybrid attacks against CI is especially important because the adversary most likely is expecting the population to panic, thus amplifying the attack. As Cedric de Coning of the Norwegian Institute of International Affairs puts it, hybrid threats are "…human-induced and designed to cause maximum social disruption."[16]

A necessary approach to countering hybrid threats against CI, therefore, requires preparing populations to understand, prepare for, cope with, and recover from disruptions of goods and services caused by these attacks. The term **societal resilience** describes the ability of populations to withstand and recover from a range of shocks, including those caused by hybrid attacks. The UN Office for Disaster Risk Reduction (UNDRR) defines societal resilience as "the ability of a community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of essential basic structures and functions."[17] Notably, building societal resilience helps prepare populations not only for hybrid attacks, but for a range of disruptions and threats, including natural disasters, pandemics, accidents, and human errors, as well as hybrid threats. Building societal resilience also extends beyond just preparing populations for hybrid attacks to CI and should include educating the population to identify and withstand mal- and disinformation, and even preparing for conventional and nuclear war.[18] In some countries, preparing populations for a range of threats to the homeland is called an "**all hazards approach**."[19] Other countries call it Total Defense, comprehensive defense, civil defense or civil preparedness.[20]

Finally, while building societal resilience is not necessarily a new concept, it is a new term that has taken on increased importance in the age of hybrid threats as a way of minimizing panic in populations and undermining the adversary's wider strategy of weakening a state and preventing it from project power.

Preparing Populations for Hybrid Attacks Against CI: The European Experience

Europe has a longstanding tradition of civil preparedness for war. During World Wars I and II, several countries took measures to prepare their populations for aerial bombardment and other activities that affected populated areas. The now ubiquitous "Keep Calm and Carry On" poster was one example the British government's efforts to prepare its population for war and to raise morale during World War II.[21] The threat of both invasion and nuclear war after World War II created a new urgency for civil defense on both sides of the Iron Curtain. Most European countries, as well as

Canada and the United States, adopted some form of civil preparedness during the Cold War and NATO requires civil defense as part of Article 3 of its Treaty.[22]

With the collapse of the Soviet Union in 1991, many European countries ended or greatly reduced their civil preparedness programs as part of the "peace dividend" that came with the end of the Cold War. However, following Russia's illegal annexation of Ukrainian territory in 2014, the EU, NATO and individual European countries began to rebuild civil defense programs in response to a revisionist Russia. In addition to calling Russia's activities "a violation of Ukraine's sovereignty and territorial integrity," then NATO Secretary-General Anders Fogh Rasmussen declared, "This is a wake-up call for the Euro-Atlantic community, for NATO, and for all those committed to a Europe whole, free and at peace."[23]

In response to Russia's illegal actions, NATO issued "The Wales Summit Declaration" and the "Joint Statement of the NATO-Ukraine Commission" in 2014, which vigorously condemned Russia's disregard for international law and called for its immediate withdrawal from Ukrainian territory.[24] The Declaration also specifically called out hybrid war and hybrid threats as activities that required more than traditional military capabilities to counter, including "enhancing strategic communications, developing exercise scenarios in light of hybrid threats, and strengthening coordination between NATO and other organisations, in line with relevant decisions taken, with a view to improving information sharing, political consultations, and staff-to-staff coordination."[25]

In 2016, at its summit in Warsaw, NATO created the "Seven Baseline Requirements" for civil preparedness to bolster Article 3 of the NATO Treaty. NATO leadership called for these changes based on "the recognition that the strategic environment has changed, and that the resilience of civil structures, resources and services is the first line of defence for today's modern societies."[26] They include:

1. Assured **continuity of government** and critical government services
2. Resilient **energy supplies**
3. Ability to deal effectively with the **uncontrolled movement of people**
4. Resilient **food and water resources**
5. Ability to deal with **mass casualties and disruptive health crises**
6. Resilient **civil communications systems**
7. Resilient **transport systems**.[27]

Following Russia's full-scale invasion of Ukraine in 2022, Christie and Berzina proposed that NATO's baseline requirements should be expanded to include three additional pillars: payment systems, data protection, and psychological resilience, including "the morale of the civilian population, its will to fight to defend the country or to volunteer in other ways, and its resilience to enemy disinformation and propaganda."[28] Christie's and Berzina's call for a psychological pillar emphasizes that populations are a key target of hybrid threats and governments need to prepare their populations to understand and defend against these threats as a matter of military preparedness for the alliance.

Simultaneous to NATO efforts, the EU began to prepare its member states for hybrid threats. These activities have included standing up a task force to support Eastern European countries, drafting the "Joint Framework on Countering Hybrid Threats," as well as the "Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats."[29] The EU has also released annual reports chronicling hybrid threats and progress in countering these activities.[30] The EU further adopted "The European Council Conclusions," which includes "the possibility for the Member

States to invoke the Solidarity Clause (Article 222 TFEU) in addressing a severe crisis resulting from hybrid activity."[31] In January 2023, the EU passed the "Directive on the Resilience of Critical Entities," which aims to bring all EU member countries into compliance with standards for assessing and protecting CI across eleven sectors: "energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, production, processing and distribution of food."[32]

Finally, the EU and NATO have created joint efforts to build resiliency, including addressing vulnerabilities posed by hybrid attacks on CI. In 2017, the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) was founded in Helsinki, Finland, as an initiative for NATO, EU and other partner nations to work together on understanding and withstanding hybrid threats.[33] In January 2023, the EU and NATO issued the Joint Declaration on EU-NATO Cooperation, followed by the "Alliance Resilience Objectives at the Vilnius Summit," which aimed "to prepare the Alliance for 'strategic shocks and disruptions;'" and the EU-NATO Task Force on Resilience of Critical Infrastructure was created to "bridge gaps between military, intelligence and law-enforcement communities, sharing best practices and enhancing situational awareness."[34]

Resilience Building in Sweden, the UK, and Romania

Alongside NATO and EU efforts to prepare countries for hybrid threats, several European countries have taken measures to realize this guidance and prepare their populations for disruptions to goods and services. Sweden, the UK, and Romania, in particular, have taken different approaches to developing resilience programs, making them ideal for comparison. Sweden is typically cited as having the longest running programs focused on preparing their population for war. Romania's resilience program is relatively new and includes government, civil society and private initiatives. And efforts to build resilience in the UK after "Brexit" include an independent organization, the National Preparedness Commission, which strives to be "non-political" in its efforts to prepare people for crises. Each country also provides variation in histories, geography, capabilities, preparedness, resources, and populations, which offers a wide variety of challenges from which to learn.

First, **Sweden** has a longstanding tradition of preparing its entire population for the possibility of invasion and war. It pioneered the concept of "Total Defence," which is "the range of activities required to prepare Sweden for war," and "involves the whole of society."[35] As a neutral country until 2024, Sweden's mindset has been one of "going it alone" or "self-sufficiency," which required it to prepare for war without the collective defensive guarantee of Article 5 of the NATO Treaty or its nuclear umbrella.

Sweden's Total Defence concept was created during World War II and expanded throughout the Cold War as a means of defending the kingdom from Soviet invasion. Total Defence was built on several core principles, including that the Swedish government was prepared to defend its people and territory in the event of war, that everyone in Sweden had a role to play in its country's defense, and that Swedes should never capitulate: "If Sweden is attacked by another country, we will never give up. All information to the effect that resistance is to cease is false."[36] Swedish citizens are, in fact, constitutionally obligated to fight and defend the nation, a principle also known as "the will to defend" (*viljan att försvara*).[37]

One way in which the Swedish government has prepared its population for war was by developing and distributing a booklet that provided guidance on what to do in the event of war or invasion. The original version, titled "If War Comes," was

developed during World War II and then updated throughout the Cold War. The booklet included descriptions of critical supplies to have on hand, basic first aid, how to address psychological stresses, how to speak to children about war, where to go in the event of an air raid, the meaning of different sirens, and emergency contacts. A copy was sent out to all Swedish Citizens in 1943, 1952, 1961, and a version was included in the back of the phone book.[38]

At the end of the Cold War, Sweden's Total Defense concept was greatly reduced as part of the post-Cold War peace dividend.[39] Several factors led to Sweden's recent efforts to rapidly rebuild its Total Defence program, including Russia's illegal annexation of Ukrainian territory in 2014; the Covid 19 Pandemic, which revealed vulnerabilities in supply chain resilience; and the need to integrate new Swedes and international residents into the Total Defence concept.[40]

In 2016, Sweden created what it calls "an action plan" for "protection of vital societal functions (VSF) and critical infrastructure." Rather than specifically name CI sectors, Sweden's action plan focuses on a functional definition of CI and its relationship to society, stating that CI is anything which, "A loss of or a severe disruption to the activity that alone or together with other similar events, rapidly leads to a serious societal emergency or crisis."[41] In other words, Sweden's approach to protecting CI focuses on the nexus between CI and how they support various societal functions.

In 2018 the Swedish government reissued its civil preparedness booklet to its entire population, now called *In Case of Crisis or War*, and updated it again in 2024 to reflect Sweden's inclusion in the NATO alliance.[42] The booklet begins by stating,

> *We live in uncertain times. Armed conflicts are currently being waged in our corner of the world. Terrorism, cyber-attacks, and disinformation campaigns are being used to undermine and influence us.*
>
> *To resist these threats, we must stand united. If Sweden is attacked, everyone must do their part to defend Sweden's independence – and our democracy.*
>
> *We build resilience every day, together with our loved ones, colleagues, friends, and neighbours.*
>
> *In this brochure, you learn how to prepare for, and act, in case of crisis or war. You are part of Sweden's overall emergency preparedness.*[43]

In 2022, following Russia's full-scale invasion of Ukraine, Sweden created the Psychological Defence Agency as a separate government entity. Its mission "covers external information influence that is directed at Sweden with the aim of harming Swedish interests. The purpose of psychological defence is to safeguard freedom of expression and open and democratic society."[44]

And in 2024, the *Försvarsmakten*, the Swedish Defense Forces, released a six-part series on YouTube in October 2024 called "*Krig i Vår Tid*," (War in Our Time), which take the viewer through the threat posed primarily by Russia, how the Swedish government and military are responding, and the need for a whole-of-society, Total Defence response to defend their country.[45]

The **United Kingdom** has also taken considerable steps to prepare its population for possible hybrid attacks to its CI (what it calls Critical National Infrastructure-CNI), following several hybrid attacks against its National Health Services and other CNI. In 2024, British Member of Parliament Pat McFadden warned that Russia could launch "unprovoked attacks against our critical national infrastructure," and it "can turn the lights off for millions of people."[46]

The British government has invested considerable energy into cybersecurity as a means of protecting CNI and other national vulnerabilities. In 2016, the same year the UK left the EU, it stood up the NCSC, which is part of the Government Communications Headquarters (GCHQ). The NCSC aims "to make the UK the safest place to live and work online and bring clarity and insight to an increasingly complex online world." To this end, the NCSC provides online resources for individuals and organizations of all sizes facing a range of cyberattacks; resources for managing online data; guidance for how to "retire digital assets;" a portal for reporting malign cyber activity; and annual reports, among other tools.[47]

Following Russia's full-scale invasion of Ukraine in 2022 and the UK's unequivocal condemnation of the invasion and support for Ukraine, the British government drafted the "UK Government Resilience Framework," which aims to address vulnerabilities and threats across the United Kingdom.[48] Building off the Resiliency Framework, the UK government began worst-case scenario planning for disruptions to electricity and gas supplies, particularly in the winter months. In 2023, it published the "British Energy Security Strategy," and its "Net Zero Strategy.[49] Some mitigation efforts include prioritizing energy sources, reopening strategic gas reserve sites, which were closed in 2017, and creating a rolling blackout schedule.[50]

Perhaps one of the most useful resources the UK has for preparing its populations for major disruptions to goods and services is the National Preparedness Commission (NPC), which was created in 2020, in the midst of the Covid-19 crisis, as "an independent and non-political body, whose fundamental objective is to promote policies and actions to help the UK be significantly better prepared to avoid, mitigate, respond to, and recover from major shocks, threats and challenges."[51] It partners with organizations from both private and public sectors and includes "senior figures from public life, business, academia and civil society with the mission of promoting better preparedness in the UK for a major crisis or incident."[52]

The NPC website includes articles and reports on seven areas of preparedness: Disaster Response; Governance and Risk Management; Government; Policy and Legislation; Organizational Preparedness; Risk or Threat Domains; and Societal Preparedness. Its mission ranges from influencing government on disaster preparedness to informing communities and individuals on best practices in preparing for a range of crises. "Making every level of government, organisation, community, household and individual better prepared will help to ensure that the whole of UK society is better able to avoid, absorb and respond to future global crises, whether predictable – a new pandemic, a massive cyber-attack, climate change – or something genuinely unforeseen."[53]

Romania is geographically and strategically important as an "eastern flank" country on the edge of Europe. As a NATO member, Romania provides critical access to the Black Sea and hosts the largest NATO base in Europe, along with several other smaller bases.[54] Romania also joined the EU in 2007 and became part of the Schengen Zone in 2025, making it politically and economically important to Europe as well.[55]

Given its strategic importance, Romania has been a persistent target of a variety of Russian hybrid threats designed to distract or weaken its support for NATO and the EU, including Russian interference in its 2024 presidential elections, which forced their high court to cancel the results and reschedule elections.[56] Romania also has experienced several largescale cyberattacks attributed to Russia, including DDoS attacks on government, military, banking and transportation websites on April 29, 2022, after Romania announced it would send aid to Ukraine.[57] And Romanian intelligence foiled a plot to physically sabotage its CI, also attributed to Russia, in January 2025.[58]

In response to this amount of nefarious activity, Romania has taken several steps to protect against hybrid threats, including against its CI. It conforms to NATO's Seven Baseline Requirements.[59] It also follows EU directives set out for CI protection; and it has drafted cyber security policies and established a clear chain of command for protecting its CI, which includes monitoring CI for threats, providing reports, and working with experts to ensure that its CI is secure.[60]

Romania has also created government departments designed to prepare for and respond to a range of disasters, including hybrid threats. The Romanian Ministry of Internal Affairs maintains the Department for Emergency Situations, which "co-ordinates the activities related to preventing and tackling emergency situations, to ensuring and coordinating human, material and financial resources which are necessary to restore normality after risk situations." It also coordinates emergency medical activities in the event of disasters.[61]

In 2021, Romania founded the Euro-Atlantic Resilience Centre (E-ARC) in Bucharest with backing from NATO and the EU. Its mission is "to take a whole-of-government approach to enhancing the resilience of our societies" and to be a center of excellence for societal resilience throughout Europe.[62] E-ARC produces reports, holds conferences, and maintains a network of experts across Europe to discuss various aspects of resilience.

In 2024, E-ARC worked with the Government of Romain to create the 32-page "Guide for Crisis Situations," a guidebook for disaster preparedness, which is available in Romanian and English.[63] The guidebook contains information on what to have on hand in case of an emergency, including food, water, medicine, cash, a whistle, and a radio, among other things.[64]

In addition to what to do in a time of emergency, the guidebook includes best practices for "cyber hygiene," including creating strong passwords, backing up information, installing antivirus software, and numbers to call in the event of a cyber incident. The guidebook stresses that "In a crisis situation, criminal groups and hostile states will attempt to take advantage of the inherent confusion and panic to steal private information or disable critical computer systems."[65]

The guidebook also provides basic information on spotting dis and mal information, stressing that "In a crisis situation, rumors and false information spread very quickly, sometimes amplified by state or non-state actors hostile to Romania with the aim of sowing panic, disrupting the intervention of the authorities and destabilizing society."[66]

Preparing Populations for Hybrid Threats Against CI

Europe and the study countries' efforts to prepare populations for disruptions of goods and services caused by attacks to CI suggest seven key takeaways:

First, it is helpful to define CI by its relationship with the population. Rather than specifically name sectors, Sweden defines CI by the critical services it provides and how disruptions of these services would affect populations, what it calls Vital Societal Functions. This functional definition helps governments understand the critical goods and services CI provides for a population and prepare them for the effects of disruptions to these goods and services.

Second, it is important to "harden" CI with good cyber strategies and defense against physical sabotage. Cyberattacks are the most significant vulnerability to CI today. Sweden, the UK and Romania have developed cyber strategies, policies and agencies for addressing cybersecurity, which should help with identifying, mitigating and recovering from cyberattacks against CI. Public-private partnerships are also important to help mitigate the gaps and seams in CI and other related cybersecurity concerns. Additionally, physical sabotage should not be overlooked as a potential hybrid attack

against CI. Defending against physical sabotage requires strengthening the physical security of CI and improving intelligence aimed at identifying saboteurs and types of attacks on CI.

Third, governments should create policies and guidelines that establish a baseline of preparedness for defending against hybrid attacks to CI and preparing for crises when defensive measures fail. Hybrid attacks on CI rarely stop at a country's borders. The EU and NATO have policies and guidelines designed to create a baseline of preparedness among member states against a range of threats, including against CI, to help mitigate disruptions of goods and services, both manmade and natural, and reduce possible "spillover" effects from one country or region to the next.

Fourth, it is necessary to physically and psychologically prepare populations for disruptions of goods and services caused by hybrid threats to CI, and to build societal resilience more broadly. These measures include informing populations of the necessary goods to have for a specified amount of time, where to go in the event of specific crises, a communications strategy in the event of cellphone disruptions, and what to do in response to specific crises. Populations also should be psychologically prepared, including understanding the intent behind hybrid attacks to CI and to preserve rather than panic, which is what the adversary wants. Put together, physically and psychologically preparing populations for the possibility of disruptions caused by hybrid attacks should reinforce one another and work to build societal resilience. Sweden and Romania have created guidebooks designed to prepare their populations for a spectrum of crises, ranging from dis- and mal-information to natural disasters to war and occupation. Sweden has mailed copies to each household to have on hand in the event of power and/or cellphone service disruption.

Finally, Non-Governmental Organizations may be useful for consistent messaging.

The UK and Romania have created independent, apolitical organizations dedicated to disaster preparedness and building societal resilience. These organizations may be helpful in providing continuity of information and messaging across administrations and in politically, ethnically and socially divided countries.

Conclusion

Hybrid threats are not going away any time soon. In fact, it is likely that adversaries will continue to use hybrid threats with increasing frequency because they are a means of offsetting the United States, NATO and other countries' conventional military capabilities without direct confrontation and attribution. The International Institute for Strategic Studies in the UK issued a report in August 2025 that enumerates Russian attacks on CI in Europe since 2022, and notes that in 2024, confirmed Russian attacks on European CI had gone up 246 percent from the previous year alone.[67] These state-driven attacks are unlikely to end, and they cannot be completely prevented. Therefore, preparing populations for the physical and psychological effects of these activities is urgently needed.

Endnotes

[1] This article is derived from the report "Preparing Populations for Hybrid Attacks Against Critical Infrastructure," published by the Irregular Warfare Center. The full report can be found at: https://irregularwarfarecenter.org/publications/research-studies/preparing-populations-for-hybrid-threats-against-critical-infrastructure-the-european-experience/.

[2] Dustin Volz, Sadie Gurman And David Uberti, "U.S. Retrieves Millions Paid to Colonial Pipeline Hackers -- 4th Update," *Wall Street Journal*, 07 June 2021.

[3] Sean Michael Kerner, "Colonial Pipeline Hack Explained: Everything You Need to Know," *Techtarget*, 26 April 2022. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know, as of 10 April 2025; and Christopher Brito, "Officials Warn People Not to Fill Plastic Bags with Gasoline Amid Panic Over Gas Shortage," *CBS Evening News*, May 14, 2021. https://www.cbsnews.com/news/gas-shortage-plastic-bags-warning-consumer-product-safety/, as of 23 April 2025.

[4] "Remarks by President Biden on the Colonial Pipeline Incident," *The White House,* May 13, 2021. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/, as of 10 April 2025.

[5] "FBI Deputy Director Paul Abbate's Remarks at Press Conference Regarding the Ransomware Attack on Colonial Pipeline," *FBI National Press Office*, June 7, 2021. https://www.fbi.gov/news/press-releases/fbi-deputy-director-paul-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline, as of 23 April 2025.

[6] "Joint Doctrine Library," *Joint Chiefs of Staff*. https://www.jcs.mil/Doctrine/, as of 24 November 2024.

[7] "Irregular Warfare 101 Course," *Defense Security Cooperation University*, https://dscu.edu/course-catalog/course/13271, as of 14 April 2025.

[8] Hybrid COE, "Hybrid Threat as a Concept." Another term used to describe this range of hostile activities is political warfare, a term used by U.S. statesman George Kennan. See: "269. Policy Planning Staff Memorandum," May 4, 1948. https://history.state.gov/historicaldocuments/frus1945-50Intel/d269, as of 21 January 2025. China uses the term "unrestricted warfare". See: Mark Thomas, "The Chinese Roots of Hybrid Warfare," *CEPA*, August 10, 2022. https://cepa.org/article/the-chinese-roots-of-hybrid-warfare/, as of 20 January 2025.

[9] Mark Galeotti, *The Weaponization of Everything: A Field Guide to the New Way of War* (New Haven: Yale University Press, 2022).

[10] Ronald Bearse, "Understanding Critical Infrastructure," pp. 1-12, in Carol V. Evans (ed.), *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency* (Carlise, PA: U.S. Army War College Press, 2022), 1-2.

[11] Carol Evans, "Executive Summary," pp. xxi-xxviii, in Carol V. Evans, ed. *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency* (Carlise, PA: U.S. Army War College Press, 2022), xxiii.

[12] See, for example: Jeff Coffed, "The Theat of GPS Jamming: The Risk to an Information Utility," *Exelis*, February 2024. https://rntfnd.org/wp-content/uploads/Exelis-GPS-Vulnerability-Assessment-February2014.pdf, as of 26 March 2025.

[13] For a scenario involving prolonged lack of electricity and its cascading effects, see: Cedric De Coning, "Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats," *Hybrid COE Working Paper No. 9*, June 2021, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-9-strengthening-the-resilience-and-adaptive-capacity-of-societies-at-risk-from-hybrid-threats, as of 28 March 2025.

[14] Mike McQuade, "The Untold Story of NotPetya: The Most Devastating Cyber Attack in History," *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, as of 23 March 2023.

[15] For NATO's definition of terrorism, see: "NATO's Military Concept for Defence Against Terrorism," 19 August 2016, https://www.nato.int/cps/en/natohq/topics_69482.htm#:~:text=The%20unlawful%20use%20or%20threatened,political%2C%20religious%20or%20ideological%20objectives, as of 22 March 2025.

[16] De Coning, "Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats," 15.

[17] "Resilience," *UNDRR*, https://www.undrr.org/terminology/resilience#:~:text=The%20ability%20of%20a%20system,and%20functions%20through%20risk%20management, as of November 23, 2024.

[18] Disinformation is incorrect information deliberately spread to cause harm. Mal-information is true information deliberately spread to cause harm, and misinformation is false information spread without the intention to cause harm. Information as HT involves intention and, therefore, disinformation and mal-information are the better terms. See: Claire Wardle, "Understanding Information Disorder," *First Draft News*, September 22, 2020. https://firstdraftnews.org/long-form-article/understanding-information-disorder/, as of 22 January 2025.

[19] Mikael Wigell, Mariette Hägglund, Christian Fjäder, Emma Hakala, Johanna Ketola, and Harri Mikkola, "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness," *FIIA Report*, No. 70, September 2022. https://fiia.fi/en/publication/nordic-resilience, as of 28 May 2025.
[20] Sweden, for example, has the concept of "Total Defence," which includes civil defense and military defense. See: "Total Defence," *Government Offices of Sweden*. https://www.government.se/government-policy/total-defence/, as of 26 March 2025.
[21] Interestingly, the poster was not widely distributed during the war. See Stuart Hughes, "The Greatest Motivational Poster Ever?" *BBC*, 4 February 2009. http://news.bbc.co.uk/2/hi/uk_news/magazine/7869458.stm, as of 3 May 2025.
[22] Article 3 of the NATO Treaty states, "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack." See: "Resilience, Civil Preparedness and Article 3," *NATO.* https://www.nato.int/cps/en/natohq/topics_132722.htm, as of 12 May 2025.
[23] Fred Dews, "NATO Secretary General: Russia's Annexation of Crimea is Illegal and Illegitimate," *Brookings,* March 19, 2014. https://www.brookings.edu/articles/nato-secretary-general-russias-annexation-of-crimea-is-illegal-and-illegitimate/, as of 3 May 2025.
[24] "Joint Statement of the NATO-Ukraine Commission," *NATO,* 4 September 2014. https://www.gov.uk/government/publications/nato-summit-2014-joint-statement-of-the-nato-ukraine-commission/joint-statement-of-the-nato-ukraine-commission, as of 30 April 2025. And "Wales Summit Declaration," *NATO*, September 2014. https://web.archive.org/web/20150621015842/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/351406/Wales_Summit_Declaration.pdf, as of 30 April 2025.
[25] Point 13, "Wales Summit Declaration."
[26] Wolf-Diether Roepke and Hasit Thankey, "Resilience: The First Line of Defence," *NATO Review*, 27 February 2019. https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html, as of 29 April 2025.
[27] Directly quoted from Roepke and Thankey, "Resilience: The First Line of Defence."
[28] Edward Hunter Christie and Kristine Berzina, "NATO and Societal Resilience: All Hands On Deck in an Age of War," *The German Marshall Fund of the United States Policy Brief,* July 2022. https://www.gmfus.org/sites/default/files/2022-07/NATO%20and%20Societal%20Resilience%20All%20Hands%20on%20Deck%20in%20an%20Age%20of%20War.pdf, as of 7 July 2025.
[29] Niklas Nilssen, et al. "Security Challenges in the Grey Zone," pp. 1-18, in Mikael Weissmann, et al (eds.), *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations* (London: I.B. Tarus, 2021), 6; and European Commission, "Hybrid Threats," *European Commission*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en, as of 4 May 2025.
[30] European Commission, "Hybrid Threats,"
[31] As quoted in Sandra Kalniete and Tomass Pildegovičs, "Strengthening the EU's Resilience to Hybrid Threats," *European View* 20, No. 1 (2021):23-33. Quote taken from p. 26.
[32] "Critical Infrastructure Resilience at EU-Level," *European Commission*, 23 September 2024. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en, as of 10 May 2025.
[33] Nilssen, et al. "Security Challenges in the Grey Zone," 6.
[34] Charlie Edwards and Nate Seidenstein, "The Scale of Russian Sabotage Operations Against European Critical Infrastructure," *International Institute for Strategic Studies*, August 2025. Quote taken from p. 12. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/, as of 26 August 2025.
[35] "Total Defence," *Government Offices of Sweden*. https://www.government.se/government-policy/total-defence, as of 29 May 2025.
[36] Alex Maxia, "Nordic Neighbours Release New Advice on Surviving War," *BBC*, November 18, 2024. https://www.bbc.com/news/articles/cjr4zwj2lgdo, as of 21 April 2025.
[37] Teemu Häkkinen and Miina Kaarkoski, "Willingness to Defend and Foreign Policy in Sweden and Finland from the Early Cold War Period to the 2010s," *Scandinavian Journal of History* 49, No. 2 (2024): 266-285.
[38] "Download or Order the Brochure In Case of Crisis or War," *Swedish Civil Contingencies Agency (MSB)*. https://www.msb.se/en/advice-for-individuals/the-brochure-in-case-of-crisis-or-war/download-and-order-the-brochure-in-case-of-crisis-or-war/, as of 30 May 2025.
[39] Karl Lallerstedt, "Rebuilding Total Defense in a Globalized Deregulated Economy: The Case of Sweden." *Prism* 9, no. 23 (2021):90-104.

[40] See, for example: Wigell, et al, "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness,"11; Fredrik Bertilsson, "The Swedish Defence Research Establishment (FOA) and the Influence of Historical Knowledge on Swedish Civil Resistance Policy," *Scandinavian Journal of History* 46, no. 4 (2021): 550-569; Lallerstadt, "Rebuilding Total Defense in a Globalized Deregulated Economy."
[41] "Protection of Vital Societal Functions & Critical Infrastructure," *Swedish Civil Contingencies Agency* (*MSB)*, July 2016. https://www.msb.se/siteassets/dokument/publikationer/english-publications/protection-of-vital-societal-functions--critical-infrastructure.pdf, as of 7 June 2025.
[42] "Download or Order the Brochure In Case of Crisis or War."
[43] "In Case of Crisis or War," 3.
[44] "Our mission," *Psychological Defence Agency (Government of Sweden)*. https://mpf.se/psychological-defence-agency/about-us/our-mission, as of 14 September 2025.
[45] "War in Our Time," *Försvarsmakten (YouTube)*, https://www.youtube.com/playlist?list=PLGXVHgImhBQI4-E55p7q8ngE_-L-GuK3g, as of 1 June 2025.
[46] Victor Jack, "UK Warning: Russia's ‚Aggressive' Cyber Warfare is Threat to NATO," *Politico*, November 24, 2024. https://www.politico.eu/article/russias-aggressive-cyber-attack-putin-poses-threat-nato-uk/, as of 3 June 2025.
[47] The National Cyber Security Centre Homepage, *Government of the UK*. https://www.ncsc.gov.uk/, as of 4 June 2025.
[48] "The UK Government Resilience Framework," *Government of the UK*. https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html, as of 4 June 2025.
[49] "Powering Up Britain: Energy Security Plan," 4 April 2023, *Government of the UK*. https://www.gov.uk/government/publications/powering-up-britain/powering-up-britain-energy-security-plan, as of 5 June 2025.
[50] Rob Hastings, "How the UK's Emergency Electricity Rationing Plans Could Work This Winter," *iPaper*, 8 October 2022. https://inews.co.uk/news/uk-blackout-plans-government-emergency-strategy-winter-electricity-rationing-1899998?ico=in-line_link, as of 5 June 2025.
[51] "About," *National Preparedness Commission*. https://nationalpreparednesscommission.uk/about/, as of 6 June 2025.
[52] "National Preparedness Commission," *LinkedIn*. https://www.linkedin.com/company/national-preparedness-commission/?originalSubdomain=uk, as of 6 June 2025.
[53] "Our Mission," *National Preparedness Commission*. https://nationalpreparednesscommission.uk/about/our-mission/, as of 6 June 2025.
[54] Madalin Necsutu, "Romania to Host Largest NATO Military Base in Europe," *Balkan Insight*, March 21, 2024. https://balkaninsight.com/2024/03/21/romania-to-host-largest-nato-military-base-in-europe/, as of 11 June 2025.
[55] "Bulgaria and Romania Join the Schengen Area," *Migration and Home Affairs*, January 3, 2025. https://home-affairs.ec.europa.eu/news/bulgaria-and-romania-join-schengen-area-2025-01-03_en, as of 11 June 2025.
[56] Rowan Ings, "The TikTokers Accused of Triggering an Election Scandal," *BBC*, 30 April 2025. https://www.bbc.com/articles/cqx41x3gn5zo as of 11 June 2025. See also: Tim Ross, "Romanian Court Cancels Presidential Elections Amid Russian Influence Fears, *Politico*, December 6, 2024. https://www.politico.eu/article/romania-court-cancels-presidential-election-runoff-tiktok-russian-influence-calin-georgescu/, as of 11 June 2025.
[57] Madalin Necsutu, "Cyber Attacks Hit Romanian Government Websites," *Balkan Insight*, April 29, 2022. https://balkaninsight.com/2022/04/29/cyber-attacks-hit-romanian-government-websites/, as of 12 June 2025.
[58] "SRI Foiled a Sabotage Operation Conducted by the Russian Federation on Romania's Territory," *SRI website*, January 17, 2025. https://www.sri.ro/articole/SRI-foiled-a-sabotage-operation-conducted-by-the-Russian-Federation-on-Romanias-territory.html, as of 12 June 2025.
[59] Marius Laurentiu Rohart, "Overview of Critical Infrastructure Protection in Romania," *The 9th International Scientific Conference* "Defense Resource Management in the 21st Century," Braşov, November 14, 2014. https://codrm.eu/wp-content/uploads/2024/12/32_Rohart.pdf, as of 12 June 2025.
[60] "Coordinating Centre for Protection of Critical Infrastructure," *Ministry of Internal Affairs of the Government of Romania*. https://www.mai.gov.ro/en/coordinating-centre-for-protection-of-critical-infrastructure/, as of 12 June 2025.
[61] "Department for Emergency Situations, Romania," *Ministry of Internal Affairs of the Government of Romania*. https://civil-protection-knowledge-network.europa.eu/organisations/department-emergency-situations-romania, as of 12 June 2025.
[62] "Euro-Atlantic Resilience Centre Mission Statement." https://e-arc.ro/en/2024/03/18/e-arc-mission-statement/, as of 3 February 2025.
[63] "Guide for Crisis Situations." *Government of Romania*, 2024. https://e-arc.ro/wp-content/uploads/2024/06/Guide-EN.pdf, as of 3 February 2025.
[64] "Guide for Crisis Situations," 14-15.
[65] "Guide for Crisis Situations," 16-17. Quote from p. 16.

[66] "Guide for Crisis Situations," 21.
[67] Edwards and Seidenstein, "The Scale of Russian Sabotage Operations Against European Critical Infrastructure,"12.

The War on Drugs

Insights from the Reagan Era

By Mark Southern

Latin America has been a hub for illicit drug production for decades, stemming from both political instability and poverty.[1] This, coupled with its proximity to the US and its high demand for South and Central American drug product, has created a parasitic yet symbiotic relationship.[2] When Richard Nixon, citing spikes in youth drug use and arrests in the 1960s, called for a national strategy to combat the influx of illegal narcotics, he set the US down a path that it still travels today, one with no apparent end or exit.[3] Despite declaring a "War on Drugs" later on, Nixon was unable to combat the problem. The Carter administration did little to help the matter, and by the time Ronald Reagan was elected in the 1980s, the problem was nearly out of control.

The purpose of this paper is to demonstrate that conditions beyond Reagan's control, and conditions fostered by his policies, were responsible for making it almost impossible for his administration to keep cocaine, and its dangerous cousin crack, from wreaking havoc in the United States. Given that the war on drugs has morphed from a police action into the "grey zone" of hybrid warfare, whereby migration has been weaponized, drones are used to survey drug or human-smuggling routes, drop improvised explosive devices and traffic illegal narcotics, and Special Operations forces are used to train local police, this paper will also provide commentary on modern efforts to fight the war on drugs.[4]

Since the Nixon Administration declared the war on drugs, it is estimated that the fight has cost his and ensuing administrations, and the American taxpayer, over one trillion dollars.[5] When one considers that modern cocaine production is at a record high, having increased by more than thirty percent since 2023 the cost seems to notably outweigh the value.[6] At no point was the war on drugs so dramatic, so violent, and so significant as it was during the 1980s. A 1988 Senate Foreign Relations report determined that the "narcotics problem is a national security and foreign policy issue of significant proportions," and that the objectives of the cartels "seriously jeopardize U.S. foreign policy interests and objectives throughout Latin America and the Caribbean."[7]

The foreign policies of the United States (U.S.) towards drug source countries clearly failed to help. At the height of Pablo Escobar's empire in the 1980s, it was estimated that the Medellin Cartel, based in Colombia, was

Mark Southern is a Royal Canadian Mounted Police officer with more than 20 years' experience investigating international cybercrime, money laundering, and drug trafficking/production offences, including methamphetamine, heroin, and cocaine. He holds a Master's degree in War Studies from the Royal Military College of Canada.

responsible for roughly eighty percent of all the cocaine shipped into the U.S.[8] Many years later, the Trump Administration's Office of National Drug Control Policy estimated that not only does over 200.000 hectares (494,210 acres) of land remain committed towards coca production in Colombia, but that the country is now responsible for *ninety* percent of all the cocaine that enters the U.S.[9] Moreover, cocaine use in the U.S. remains high, with five million Americans reporting as having used it as recently as 2020.[10] Not coincidentally, the number of American deaths related to cocaine, according to the Drug Enforcement Administration's (DEA) 2020 National Drug Threat Assessment, has more than *tripled* since 2010.[11]

What went wrong?

Nixon declared the "all out, global war" on drugs in a message to Congress on March 28, 1973, claiming that increasing crime rates, and the destruction of American lives, were the direct result of increased drug use amongst U.S. citizens.[12] As cocaine slowly began to grow in popularity, the war on drugs continued through the Ford and Carter administrations, and the latter's redirected focus towards harm-reduction, including hospitalization and treatment, while wonderful for addicts, did little to combat the influx. Ronald Reagan came into office with a renewed zeal to fight the war on drugs.[13] However by the end of his two terms, cocaine, heroin, and marijuana were *all* more readily available in the U.S. than when he was elected eight years prior.[14]

Did he fight a good fight? Did his actions and policies help?

Condition #1 - Inheriting an Already Bad Situation

The DEA, which was created pursuant to Nixon's 1973 *War* declaration, emerged from the earlier Bureau of Narcotics and Dangerous Drugs (BNDD) into a "superagency" responsible for coordinating all federal efforts related to drug enforcement.[15] In its early years much of its efforts were directed towards heroin and marijuana.[16] The increase in use of marihuana from the 1960s into the 1970s is sufficiently attributable to loosening norms and a growing youth counterculture.[17] The spike in heroin use is from something slightly darker. Due to the ease with which it was obtainable in southeast Asia, it is estimated that that eighty-thousand U.S. servicemen in Vietnam had tried heroin, and Congressional findings determined that 10-15 percent of these returned to the U.S. as addicts.[18]

The DEA identified Mexico as the source country for the majority of heroin and marijuana entering the U.S., and through the early to mid-1970s, engaged in successful poppy and marijuana eradication campaigns in that country.[19] These eradication operations in the Northern Mexican states of Chihuahua, Durango, and Sinaloa, coupled with tighter border security spoken to in Nixon's declaration, essentially locked down production capabilities for the Mexican smugglers. Recognizing the opportunity, Colombian traffickers filled the vacuum and began growing what the DEA would later refer to as "Colombian Gold," and this in turn shifted the epicenter of marijuana production from northern Mexico to Colombia, to the point where by the end of the 1970s, Colombia was responsible for 70 percent of the marijuana that reached the U.S.[20] A 1988 Senate Foreign Relations report concluded that *this* shift in turn resulted in the creation of a "criminal narcotics infrastructure…in both Colombia and the United States."[21] The resulting "marijuana complex" became both highly organized and lucrative, engendering a new moneyed elite, and proved critically important to the Colombian economy, with 30,000-50,000 farmers dedicated to cultivation, and close to 50,000 *additional* seasonal workers, traffickers, security, and financiers involved in the production process.[22]

At the same time, General Augusto Pinochet overthrew Salvador Allende's government in Chile. Allende's Popular Unity government was attempting a program of nationalizing resources and redistributing income, and fearing losing Chile and potentially other Latin American nations to Soviet influence, which would in turn risk harming the interests of several multinational corporations supportive of the Republican administration, Nixon, his secretary of State Henry Kissinger, and the Central Intelligence Agency (CIA) orchestrated a coup on September 11, 1973 to bring Pinochet's military government into power.[23]

Chile had by then become an important smuggling corridor for cocaine produced in Bolivia and Peru "the pioneers" and original traffickers of cocaine according to Paul Gootenberg, who by the 1960s had put in place the framework to traffic hundreds of kilograms of cocaine a year to the U.S.[24] Pinochet aggressively pursued the traffickers, which disrupted the regional networks. Interestingly, in a later statement to the Chilean courts, former aide Manuel Contreras alleged that Pinochet and his son later actually took control of the network, organized a massive production program, and sold cocaine to Europe and the U.S., amassing a fortune worth twenty-six million dollars.[25]

Nonetheless, Pinochet's crackdown created the ideal opportunity for a group of Colombians from Medellin–marijuana-complex, moneyed elite drug traffickers--to take control, and once they did, they would leverage that network into one that would yield hundreds of *tons* a year the mid 1980s.[26]

The above-noted conditions paved the way for cocaine replacing any other narcotic in popularity in the U.S.[27] Miami became the drug capital of the Western Hemisphere due primarily to its geography, and southern Florida was assaulted by a wave of violence related to the cocaine trade.[28] From seizures of 108 pounds of cocaine in 1970, in 1975 the U.S. Customs Service seized 729 pounds, and in the Miami Airport alone, seizures increased from 37 pounds to 271.[29] More alarmingly, 50 percent of Miami's homicides during the late 1970s were drug-related, and the spike in murders essentially collapsed the morgue system in that city.[30] These are the conditions inherited by the Reagan administration, and foreign policies from earlier administrations, whether unknowingly or not, clearly played a role. Reagan cannot be faulted for these conditions, but would his policies help mitigate the situation?

Condition #2 - Reaganomics and the Popularity Of Cocaine

The U.S. economy in the 1970s was suffering from high unemployment and high inflation, the combined rates of which Jimmy Carter referred to as the "Misery Index," which stood at 13 percent on the day he was elected, and 21 percent four years later.[31] Reagan came into office hoping to help the U.S. escape from the disastrous recession that had befallen the economy in the 1970s.[32] His resulting program was based on supply-side economics–essentially lowering tax rates so people retained more of their earnings, proponents of which argued that more money in hand results in greater savings and investment, and therefore greater overall economic growth.[33] By the end of *his* two terms, twenty million new jobs had been created, the Misery Index dropped to 11.7 percent, and middle-income family earnings rose by 27 percent.[34] Combine this with the maturation of the youth counterculture, and its laissez-faire attitude towards drugs, from the 1960s and 70s into the 1980s, and an observable increase in drug use seems plausible; a demographic inured to drug use, now with more money. What made the increased use of cocaine *probable* however, was the pronouncement by Carter administration drug advisor Dr. Peter Bourne that not only was cocaine *not* addicting, it was "acutely pleasurable."[35] This probability is demonstrated by the fact that by

1979, a national survey of 18 to 25 year-olds taken in 1979 resulted in admissions that 70 percent had taken illegal drugs, 50 percent were regular drug users, and at least 20 percent were using cocaine.[36]

The glut of cocaine flooding the U.S. markets through the port of Miami caused the street level per-gram price to progressively fall from roughly $750 in 1981 to roughly $300 by 1987.[37] So, with the federal government having righted the economy, the counterculture youth maturing into adulthood and more disposable income in their pockets, and the perception that cocaine was not addictive and almost recommended by the outgoing Democratic administration, it is not at all surprising that cocaine use skyrocketed, in both white collar circles, as its use became "chic," and in inner cities in its cheaper and more addictive form, crack, cocaine mixed with baking soda and heated until it solidifies.[38]

Again, Reagan can hardly be faulted for the restoration of the American economy. Still, as crime and addiction rates were rising, his response to combating the drug problem would certainly be measured with great scrutiny.

Condition #3 – A Careless War Effort

Reagan quadrupled funding for fighting the influx of cocaine from $416 million in 1981 to $1.6 billion by 1987, and the focus of the U.S. was directed at the coca-rich Andean region encompassing Colombia, Bolivia, and Peru.[39] Consistent with previous programs, eradication and interdiction were the Reagan administration's mainstays.[40]

Eradication

Fortunately for the Medellin Cartel, neither did the U.S. State Department even request funding for the continued "aerial eradication of illicit drug crops," nor did the Colombian government begin focusing efforts on herbicide campaign of aerial spraying, until 1986.[41] For nearly three-quarters of Ronald Reagan's full term in office, no efforts were made to eradicate coca plants in Colombia.

Mathea Falco emphasized that even when the eradication campaign began, several key factors hindered it further. For one, Bolivia and Peru both lacked a strong government, and this translated into the absence of control and direction in the coca-growing areas.[42] In Colombia, not only was local political support in the growing areas secured through bribery and intimidation, but the cartels themselves possessed better equipment and weaponry than any military or police units.[43] When the eradication campaigns finally began, the previously impoverished farmers, now recognizing regular incomes from coca relative to coffee, corn or potatoes, became "fiercely resistant" to government authorities, and if police *did* intervene, cultivation moved deeper into the jungles into previously unused areas.[44] This is undoubtedly due to the loyalty engendered by Escobar in his native Colombia. He was shielded by a group of supporters for whom he had built houses, hospitals and sports facilities, provided jobs and raised incomes.[45]

Another reason complicating matters early for Reagan was the election of Belisario Betancur in 1982. The conservative president stated that he had no intention of Colombia becoming a satellite of the U.S.[46] Narcotics notwithstanding, he was also critical of Reagan's trade and economic policies, stating that the U.S. was becoming increasingly protectionist, and was refusing to increase its International Monetary Fund contributions, which was causing Colombia and other Third World countries to suffer.[47] Belisario's term ended in 1986, so for a good portion of Reagan's presidency, he clearly did not have an ally in Colombia with whom Washington could entrust an effective eradication program.

Foreign policies notwithstanding, the obvious result was that Escobar and his associates had what must have seemed to them a limitless supply of coca

with which to fill their massive inventory of finished drug product.

Interdiction

Reagan undertook the largest drug interdiction campaign in U.S. history, but the results here were also less than stellar.[48]

Due to the porous conditions at the port of Miami, through which a majority of the cocaine was coming, the South Florida Task Force was established in 1982, chaired by Vice-President George H. W. Bush and comprised of units from the Coast Guard, DEA, Customs, and Treasury.[49] Granted, any measurement of success one year into his presidency might be difficult to arrive at, but the U.S. General Accounting Office report determined that in 1983, *more* drugs were entering the country than five years prior, and a second report in 1985, indicated the problem was worsening.[50] Falco again provides some insight. A major component of the interdiction strategy focused on marijuana.[51] This likely seemed an "easy score," and increased seizures would certainly demonstrate that the interdiction program was working. The increased enforcement focus on marijuana, however, encouraged traffickers simply to switch to cocaine.[52]

The Medellin cartel was trafficking cocaine by freighter, large and small aircraft, mini-submarine, and speedboat, and by the time Reagan was seeking re-election, this amounted to two tons of cocaine *weekly*.[53] There is arguably little in the way of money, resources, tools or enforcement personnel that could ever have made an impact on this. In October 1986 the task force boasted that it had seized 4,620 *pounds* of cocaine from a freighter near Miami, and that this was the "largest confiscation" in U.S. history.[54] That result, given the weekly *tonnage* from Medellin, is nothing short of laughable.

A 1986 statement to the *Washington Post* by Democratic Representative Glenn English, chairman of the House Government Operations oversight subcommittee which held thirty-eight hearings into the federal government's drug eradication and interdiction program, provides additional insight. English indicated that the U.S. Coast Guard had "only a handful of poorly equipped and undermanned boats available for drug efforts in South Florida" to deal with "3,600 boatloads of cocaine."[55] He further stated that "on the entire West Coast there are only eight Customs boats and most of those can't leave the harbor," and the that the situation in the air was much worse. It was estimated that flights in which drugs were smuggled would number approximately 18,000 in 1986, but the U.S. Customs Service "has only six aircraft to intercept and follow planes carrying illegal drugs and only eight helicopters to carry law enforcement officials to arrest smugglers."[56]

Both the DEA and Customs officials made public their dissatisfaction. Gerald Hochman, who led the DEA component of the South Florida Task Force said that "We'd like to have impacted more, but we haven't. I'd like to say that we are at least containing the problem, but I am not even sure that is accurate." George Heavey, the regional Customs commissioner added, "We're overwhelmed. It's like fighting the Chinese Army."[57]

Where the $1.6 billion endowed by Reagan to fight the onslaught of smuggling landed, if *not* in the hands of those tasked to fight it, begs serious further investigation. Nonetheless, the result was a country with many wealthy and poor, black and white, indiscriminate citizens with a demand for cocaine in all its forms, and a supply that was cheap and plentiful, and little being done in the way of enforcement to stop it. An examination of Reagan's larger foreign policies in Latin America will shed some light on this seemingly lax attitude towards the war on drugs.

Condition #4 – Weak Latin American Policies

The Carter administration's negotiation of a new Panama Canal Treaty, originally orchestrated under Nixon, not only ended U.S. control of the strategic waterway, but it was also a symbolic

gesture to the rest of Latin America of a more cooperative stance by the U.S., with a greater emphasis on human rights. This softened stance came with a decrease in support for right-wing military regimes, such as Pinochet's in Chile, as well as the Somoza government in Nicaragua.[58]

Anastasio Somoza had been a close U.S. ally, but Carter's soft approach, coupled with corruption within Somoza's government, destabilized the country, and created violent opposition culminating in a civil war. This resulted in *Sandinista* guerillas--avowed Marxist-Leninists and Soviet and Cuban allies--seizing control of the government in 1979.[59] The Reagan Doctrine countering soviet influence from "Afghanistan to Nicaragua" was clear on U.S. Central American foreign policy in the 1980s. A focus on not only containing, but pushing Soviet influence back, particularly in the developing world would blind the Reagan administration to Medellin cartel's ambition.[60]

Fearing further Soviet encroachment in the region, the Reagan Administration funded and supplied anti-Sandinista fighters, referred to as *Contras*, throughout much of the 1980s.[61] Whether due to willful blindness or sheer ignorance on the part of the U.S. government, a 1989 Senate Committee on Foreign Relations report concluded that during most of Ronald Reagan's presidency, the Contras not only participated in narcotics trafficking but also received money, weapons, aircraft, and pilots from drug traffickers. Even more troubling, funds authorized by Congress for Contra humanitarian aid were diverted into the hands of those traffickers.[62] Further, General Paul Gorman, then head of the U.S. Army's Southern Command, responsible for Central America, testified that "the use of narcotics profits by armed resistance groups was commonplace," and DEA testimony indicated that weapons for the Contras made their way to Nicaragua from Panama "on small planes carrying mixed loads, which included drugs. The pilots unloaded the weapons, refueled, and headed north toward the U.S. with drugs."[63] So very clearly, under the nose of the U.S. government, the flow of cocaine occurred with ease through Nicaragua, a country receiving a substantial amount of American tax dollars.

More embarrassingly, the Senate committee determined that the above-noted Panama link was facilitated by corrupt Panamanian government officials, and that the failure of the U.S. to deter this association was "largely the result of the relationships Panamanian officials had developed with U.S. intelligence and law enforcement agencies."[64] This is undoubtedly referring to Manuel Noriega, who allowed U.S. listening posts to be set up in Panama, allowed the country to be utilized as a conduit for U.S. money and weapons into Nicaragua, and who assisted the Reagan administration as they "sought to undermine the Sandinistas."[65] Someone, somewhere in the American hierarchy had overlooked that fact however, because as early as the beginning of the 1970s, the DEA's predecessor, the BNDD, identified Noriega as undeniably "working with traffickers".[66] As he consolidated his power into the early 1980s and the narcotics situation in Panama worsened, Noriega then took control of the country's most important institutions, and utilized them to exercise control over the drug trade.[67] What this amounted to by 1982 was that Noriega was working closely with the Medellin cartel on several fronts. The committee noted that "First, he was laundering their drug money. Second, he permitted the cartel to establish processing plants in Panama,"[68] Worsening matters even further, the DEA developed and maintained a long-standing relationship with the Panamanian Defense Forces pertaining to drug investigations, money laundering, crop eradication, and interdiction. The closeness of this relationship enabled Noriega to obtain intimate and sensitive information, which he is believed to have shared with the cartel.[69] The committee concluded that the U.S. government "did nothing regarding Noriega's

drug business and substantial criminal involvement because the first priority was the Contra War."[70] Noriega recognized that helping the U.S. with their *highest* diplomatic priority–communist containment–would cause them to willingly overlook his involvement in their *lesser* priorities, including the war on drugs.

Similarly, as Honduras served as an exile destination and training ground for the Contras., U.S. military aid there was significant. In 1985, $73.9 million was sent from the U.S. to the Honduran government.[71] At the same time however, the Medellin cartel was utilizing the same Honduran ports and airstrips used by earlier Marihuana traffickers, to transfer load and refuel.[72] The Senate committee found that this was allowed to transpire due to Noriega's involvement leveraging the relationships he had developed with Honduran military intelligence officials into years' worth of cocaine-trafficking protection by the Honduran military.[73] When one of these officials later became involved in a "narco-terrorist plot" to murder then Honduran president Roberto Cordova, the U.S., in a blatant display of placing communist containment concerns over the war on drugs, "interceded in an effort to get his sentence reduced."[74] Confusingly, the committee also found that when the DEA had an opportunity to legitimately attack the drug problem in Honduras, particularly given the substantial foreign aid payments, Washington instead *closed* the DEA office in Tegucigalpa, and "ignored the issue."[75] Again, Reagan cannot be held personally responsible for this oversight, but in Honduras as well as Nicaragua and Panama, the policy of communist containment clearly outweighed the government's interest in fighting cocaine shipments.

So too, with Cuba. Multiple American law enforcement agencies further reported the routine use of Cuban airspace and territorial waters by drug traffickers as safe havens in the 1980s, sanctioned by Cuban authorities.[76] Similarly, in June, 1989 Havana reported that several high-ranking members of the Cuban military were suspected of having worked with the Medellin cartel to smuggle six tons of cocaine into the U.S.[77] The only policies directed at Cuba during this time however, were limited to 1982 travel restrictions between the two countries, a 1984 bilateral agreement to normalize immigration procedures and a 1985 arrangement to facilitate radio American radio broadcasts.[78] No mentions of anti-drug policies are made, despite the clear fact that the Medellin cartel was using the Soviet-backed close neighbour of the U.S. to move cocaine through the Caribbean. Cuba being "Soviet-backed" was likely as far as a Cold-War president's thought process would reach, and this mentality therefore served as an additional shield for the Medellin cartel.

Even in countries where the threat of Soviet influence was minimal, U.S. anti-drug policies were insufficient. In the Bahamas, sanctuary was ensured for traffickers through bribery, and Medellin associates purchased substantial tracts of land to facilitate illicit drug movement.[79] The U.S. response here was ineffective due to several key failings. First, a Senate investigation determined that any policy designed to deal with trafficking did not originate from the White House It was left to the Embassy, and any anti-drug policy made by the ambassador was not carried over to their successors. The result was that the "decreased attention to the problem went largely unnoticed in Washington."[80] The absence of coordination between the embassy and US attorneys exacerbated this case particularly in Miami, which in turn "led law enforcement officials to believe there was little point in pursuing cases against Bahamian citizens or government officials."[81]

Reagan's Caribbean Basin Initiative, an economic development program designed to stimulate growth in the region, created some hope in other countries such as Jamaica, the Dominican Republic and Haiti. The overwhelming financial problems

of these countries however, including heavy foreign debts, minimal historic growth, high levels of both inflation and unemployment, and exports insufficient to pay for imports, led to the exodus of many white-collar citizens of those nations, which cyclically worsened the problem, and led Sir Philip Sherlock, founder of the Association of Caribbean Universities and Research Facilities, to opine that "the drive for economic and social development has been frustrated by events beyond out control" and further, that "the mood has turned sour."[82]

The totality of the foregoing offers little evidence to support the fact that the Reagan administration was taking the weekly shipments of tons of cocaine with the degree seriousness and urgency such a problem warranted, despite Nancy Reagan's "Just Say No" campaign If they *were* taking such a threat seriously, it seems they were comfortable with what seems to have been perceived as an acceptable degree of loss in the war on drugs, at the mercy of communist containment. This severe lack of due diligence by Washington, and the overemphasizing of anti-communist policies over those of the war on drugs, undoubtedly made the Medellin cartel's job of moving cocaine through the Caribbean that much easier.

Nixon's declaration of a war on drugs created the DEA, who shut down marijuana production in Northern Mexico. The epicenter of production moved to Colombia, and when the U.S.-sanctioned coup in Chile forced pioneering cocaine traffickers out, the Colombians recognized the exponential profit margins from cocaine and began pumping tons of it over the U.S. borders. Reagan didn't create any of that. He inherited an already-bad situation. When he took office, his economic strategy for the U.S. created wealth for many citizens, and the view of cocaine as a benign substance, amongst a population of young Americans who had experienced a "normalization" of drugs over two decades, coupled with the benefits of Reaganomics, created the conditions for an increased demand for cocaine, and crack.

As far as actually fighting the war on drugs, as noted earlier, for a great portion of his presidency, there was little or no eradication of Colombia coca taking place. Similarly, interdiction results were equally poor. The sheer volume of *legal* global trade makes it such that only two percent of all cargo is ever subject to an inspection.[83] Anyone in Washington who believed interdiction would work against the volume of Medellin cartel shipments were therefore fooling themselves, and, also as stated earlier, with limited assets available to those on the ground in Miami, and cocaine use rising along with crime rates, Reagan's drug war effort should be viewed as deeply substandard.

With no degree of legitimacy can anyone state that Reagan was aware of what was transpiring, but the above-noted reads like the U.S. did essentially turn a blind eye to narcotics trafficking, at the mercy of other foreign policy concerns. Primary amongst these was communist containment, starting with the Nixon-assisted Pinochet coup. A weakened stance by Jimmy Carter created destabilized governments in Central America and gave Reagan the perfect opportunity to put his doctrine into practice. Given the magnitude of that--stopping Soviet aggression at America's doorstep-- it is not difficult to see that his foreign policies towards Central America caused Washington to overlook the fact that the Medellin cartel was utilizing these countries with almost free range to help get cocaine into the ripe U.S. market. These conditions made it difficult for the Reagan administration to counter the constant inflow of cocaine.

Current commentary

The foundation laid by Reagan-era policies haunts U.S. narcotics policy and operations today. Consider that since the Nixon administration the trillion dollar bill the American government has incurred,

spent on everything from DEA operations, border surveillance, public-awareness campaigns, and military aid packages to Latin America, cocaine production and consumption continue to rise.[84] That cocaine use is still a large problem is evidenced by the second Trump Administration's claim that cocaine shipments from South America are responsible for the current drug overdose problem in the U.S.[85] Keeping cocaine and crack out and off the streets of U.S. cities remains as much an impossibility now as it was twenty-five years ago. It is still one of the most widely used illicit drugs in the world, with consumers numbering in excess of twenty million, most of whom are in North America and Europe.[86] The situation is due primarily to lower costs of production, which has fueled falling street prices,[87] and that fact that in the past ten years cocaine supply chains have been greatly diversified.[88] These are beyond the control of the current or any U.S. administration, as is the fact that the prevalence of cocaine and its use in America is not a *matter* of supply–the problem is that, since Ronald Reagan's presidency, the consumer demand for powdered cocaine "has hardly blinked."[89] The difference today is the fact that modern drug production and trafficking constitutes a form or irregular warfare with many terrorist organizations relying on criminal conduct to support their activities, including drug trafficking, human trafficking, sex trafficking, and money laundering.[90] Conversely, the U.S.' recent strikes on Venezuelan vessels in the Caribbean, which have fueled significant debate concerning the authority of a state to engage in extrajudicial violence, nonetheless demonstrate that the nature of such actions now approach "combat,", as opposed to "law enforcement." This is consistent with the growing "grey zone" that has developed as the distinction between "warrior" and "organized criminal" has been blurred.[91]

Despite that fact that the criminal organization targeted by the U.S. is violent and engaged in a wide range of criminal activity including drug trafficking, it is not a major threat on the international stage, and not on a par with either ISIS or al-Qaeda.[92] Their actions are highly destabilizing however, and the act of *identifying* the group as terrorists has allowed the U.S. to normalize extrajudicial violence in the name of national security.[93] The architects of Reagan-era interdiction would no doubt wonder at the gravity of the increase in pressure the second Trump administration has placed on narcotic trade routes. The U.S. has deployed several B-52 long-range strategic bombers capable of carrying and deploying conventional and nuclear weapons to the Venezuelan coast, and they have increased their naval presence in the Caribbean, deploying Arleigh Burke-class destroyers USS Gravely, USS Jason Dunham, and USS Stockdale, the littoral combat ship USS Minneapolis-Saint Paul, as well as amphibious ships USS Iwo Jima, USS San Antonio, and USS Fort Lauderdale, the nuclear-powered fast-attack submarine USS Newport News.[94] These air and naval detachments have also been accompanied by ten thousand U.S. troops.[95] This is not law enforcement, it is a hybrid or "gray zone" warfare approach to dealing with matters that are similarly "gray" in nature, and given that fact, what is the second Trump administration to do?

The Maduro regime in Venezuela's was waging a gray zone war against the U.S. and its neighbours through irregular warfare destabilization mechanisms, including not only drug trafficking, but forced migration, and the use of criminal gangs embedded in the U.S. who serve as state semi-proxies as well.[96] Given this fact, the strategies employed to combat cocaine trafficking are necessarily different than they were in the 1980s. The fact that the tactics, strategies, and organization of modern drug cartels have grown to be perfectly consistent with those of recognized terrorist organizations has

caused a change in policy and the way governments must deal with what has morphed from drug trafficking to narco-terrorism.[97]

No dissimilar to the 1980s, cocaine use in the 2020s remains a demand problem, and that fact is beyond the control of legislators and strategists in the U.S. and elsewhere in the West. Policies and tactics employed to fight cocaine trafficking have changed over that time frame, although whether employing a hybrid warfare approach against drug shipments will prevent *further* shipments, remains to be seen.

Endnotes

[1] Isabela De los Rios Hernandez, "Knowledge, Soil, Politics, and Poverty: How Drug Trafficking Has Kept its Hold on Latin America," *The Harvard International* Review, June 26, 2024, https://hir.harvard.edu/knowledge-soil-politics-and-poverty-how-drug-trafficking-has-kept-its-hold-on-latin-america/.
[2] Hugo Balta, "Washington Loves Blaming Latin American for Drugs – While Ignoring the American Appetite that Fuels the Trade," *The* Fulcrum, January 13, 2026, https://thefulcrum.us/ethics-leadership/us-drug-crisis-latin-america-hypocrisy.
[3] NPR, "Timeline: America's War on Drugs," *NPR*, April 2, 2007, https://www.npr.org/2007/04/02/9252490/timeline-americas-war-on-drugs#:~:text=July%2014%2C%201969:%20In%20a,efforts%20of%20all%20other%20agencies.
[4] Brandon Schingh, "Using Special Operations Forces to Counter Mexican Cartels: An Irregular Analysis," *Small Wars Journal*, February 26, 2025, https://smallwarsjournal.com/2025/02/26/using-special-operations-forces-to-counter-mexican-cartels-an-irregular-analysis/.
[5] Betsy Pearl et al, "Ending the War on Drugs: By the Numbers," *The Center for American Progress*, June 17, 2018, https://www.americanprogress.org/article/ending-war-drugs-numbers/#:~:text=Researchers%20and%20policymakers%20alike%20agree,not%20a%20criminal%20justice%20issue.
[6] Robert Muggah, "The Geopolitics of Trump's War on Drugs," *America's* Quarterly, September 18, 2025, https://americasquarterly.org/article/geopolitics-war-on-drugs/.
[7] United States Senate, "Drugs, Law Enforcement and Foreign Policy," *Senate Committee on Foreign Relations, Subcommittee on Terrorism, Narcotics and International Operations*, April 13, 1989, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB113/north06.pdf. p.2.
[8] Insight Crime, "Pablo Escobar," *Insight Crime*, August 30, 2021, https://insightcrime.org/colombia-organized-crime-news/pablo-escobar/.
[9] Sergio Guzman, "4 reasons Trump's frustration about cocaine may make him pick a fight with one of the US's best friends," *The Business Insider*, July 20, 2019, https://www.businessinsider.com/4-reasons-trump-could-decertify-colombia-over-coca-cocaine-production-2019-7.
[10] The Addiction Center, "Statistics on Addiction in America," *The Addiction Center*, accessed on August 25, 2025, https://www.addictioncenter.com/addiction/addiction-statistics/.
[11] United States Department of Justice, "2020 National Drug Threat Assessment," *U.S. Department of Justice,* March, 2021, https://www.dea.gov/documents/2021/03/02/2020-national-drug-threat-assessment.
[12] The White House, "Reorganization Plan Number 2 of 1973," *The White* House, March 28, 1973, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title5a-node84-leaf182&num=0&edition=prelim.
[13] Michelle Getchell, "The Enduring Legacy of Reagan's Drug War in Latin America," *War on the Rocks,* December 20, 2018, https://warontherocks.com/2018/12/the-enduring-legacy-of-reagans-drug-war-in-latin-america/.
[14] Bruce Bagley, "US Foreign Policy and the War on Drugs: Analysis of a Policy Failure," *The Journal of Interamerican Studies and World Affairs,* Volume 30, No. 2/3, Summer/Autumn 1988, Cambridge University Press, https://www.jstor.org/stable/165986, p.189.
[15] The White House, "Reorganization Plan Number 2 of 1973."
[16] The Drug Enforcement Administration "History: The DEA Years 1970-1975," accessed August 27, 2025, https://www.dea.gov/about/history, pp. 40-45.
[17] Ben Lesser, "The History and Use of Marihuana in Society," *Dual Diagnosis,* March 16, 2021, https://dualdiagnosis.org/marijana-treatment/reefer-madness-look-evolution-marijuana-society/.
[18] Van T. Nguyen, et al, "Drug Abuse in Vietnam: A Critical Review of the Literature and Implications for Future Research", *Addiction,* Volume 103, Issue 4, April 2008, https://pubmed.ncbi.nlm.nih.gov/18261190/, p.536.
[19] The Drug Enforcement Administration "History: The DEA Years 1970-1975," pp.42-45.
[20] Steve Hyland, "The Shifting Terrain of Latin American Drug Trafficking", *Origins: Current Event in Historical Perspective, Ohio State University*, September 2011, accessed on August 20, 2025, https://origins.osu.edu/article/shifting-terrain-latin-american-drug-trafficking?language_content_entity=en.
[21] United States Senate, "Drugs, Law Enforcement and Foreign Policy," p.27.
[22] Ibid.
[23] Paul Cantor, "The Puppet and the Puppeteer," *Counterpunch*, December 16, 2006, https://www.counterpunch.org/2006/12/16/the-puppet-and-the-puppeteer/.
[24] Paul Gootenberg, "The Pre-Colombian Era of Drug Trafficking in the Americas: Cocaine: 1945-1965," *The Americas,* Vol. 64, No.2, October 2007, https://www.jstor.org/stable/30139084?seq=1, p.133.
[25] Jonathan Franklin, "Pinochet Sold Cocaine to Europe and the US," *The Guardian,* July 11, 2006, https://www.theguardian.com/world/2006/jul/11/chile.drugstrade.

[26] Hyland, "The Shifting Terrain of Latin American Drug Trafficking;" Gootenberg, "The Pre-Colombian Era of Drug Trafficking in the Americas: Cocaine: 1945-1965," *The Americas*, p.133.
[27] Jason Ferris, et al., "Weekly Dose: Cocaine, the Glamour Drug of the '70s is Making a Comeback," *The Conversation*, March 8, 2018, https://theconversation.com/weekly-dose-cocaine-the-glamour-drug-of-the-70s-is-making-a-comeback-88639.
[28] The Drug Enforcement Administration "History: The DEA Years 1970-1975," p.44.
[29] Ibid.
[30] Hernandez, "Hernandez, "Knowledge, Soil, Politics, and Poverty: How Drug Trafficking Has Kept its Hold on Latin America."
[31] Chester Pach, "Ronald Reagan and Supply-side Economics," *The Bill of Rights Institute,* accessed on August 24, 2025, https://billofrightsinstitute.org/essays/ronald-reagan-and-supply-side-economics.
[32] Mike Moffat, "The 1980s American Economy," *ThoughtCo.,* July 28, 2019, https://www.thoughtco.com/us-economy-in-the-1980s-1148148.
[33] Ibid.
[34] The Reagan Foundation and Institute, "The Second American Revolution: Reaganomics," *The Reagan Foundation and Institute*, accessed on August 24, 2025, https://www.reaganfoundation.org/ronald-reagan/the-presidency/economic-policy/.
[35] Charles Krauthammer, "Stigmatize Drug Use…," *The Washington Post*, September 8, 1989, https://www.washingtonpost.com/archive/opinions/1989/09/08/stigmatize-drug-use/5686a4a3-5d6f-42c0-83ba-9b874cbf09ed/.
[36] Michael Hedges, "'Benign' Drug of the '70s is a Scourge in the '90s," *Deseret News*, August 24, 1999, https://www.deseret.com/1999/8/24/19462324/benign-drug-of-the-70s-is-a-scourge-in-the-90s/.
[37] Christopher Woody, "Here's What's Driven Changes in Cocaine Prices on US Streets Since the 1980s," *Business Insider,* October 26, 2016, https://www.businessinsider.com/us-cocaine-prices-change-2016-10.
[38] National Public Radio, "How Americans Said No to Cocaine After Years-Long Addiction," *NPR,* July 27, 2013, https://www.npr.org/2013/07/27/206148964/how-americans-said-no-to-cocaine-after-years-long-addiction.
[39] Mathea Falco, "U.S. Drug Policy: Addicted to Failure," *Foreign Policy,* no. 102, spring 1996, https://www.jstor.org/stable/1149263, p.122.
[40] Falco, "Foreign Drugs, Foreign Wars," *Daedalus*, Vol. 121, no. 3, summer 1992, https://www.jstor.org/stable/20027119?seq=1, p.1.
[41] Joseph Weir, "The Aerial Eradication of Illicit Coca Crops in Colombia, South America: Why the United States and Colombian Governments Continue to Postulate its Efficacy in the Face of Strident Opposition and Adverse Judicial Decisions in the Colombian Courts," *Drake Journal of Agricultural Law*, Volume 10, 2005, p.212, https://nationalaglawcenter.org/wp-content/uploads/assets/bibarticles/weir_aerial.pdf.
[42] Falco, "Foreign Drugs, Foreign Wars," pp.3-4.
[43] Ibid, p.4.
[44] Ibid.
[45] Richard Boudreaux, "Talent For Business, Violence Brought a Fortune in Drug Money: Cocaine," *Los Angeles Times*, June 20, 1991, https://www.latimes.com/archives/la-xpm-1991-06-20-mn-1447-story.html.
[46] Bruce Bagley et al, "Colombian Foreign Policy in the 1980s: The Search for Leverage," *Journal of Interamerican Studies and World Affairs,* Volume 27, No. 3, Autumn 1985, https://www.cambridge.org/core/journals/journal-of-interamerican-studies-and-world-affairs/article/abs/colombian-foreign-policy-in-the-1980s-the-search-for-leverage/158F12C007058EB3F90148779839B03D, p.32.
[47] Ibid.
[48] Falco, "Foreign Drugs, Foreign Wars." p.4.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Lenny Flank, "The Cocaine King: Pablo Escobar and the Medellin Cartel," *Hidden History*, July 29, 2015 https://lflank.wordpress.com/2015/07/29/the-cocaine-king-pablo-escobar-and-the-medellin-cartel/.
[54] George Volsky, "4,620 Pounds of Cocaine is Confiscated in Florida," *The New York Times,* October 30, 1986, https://www.nytimes.com/1986/10/30/us/4620-pounds-of-cocaine-is-confiscated-in-florida.html.
[55] Bill Peterson et al, "Drug Interdiction Effort a Failure, Governors Told," *The Washington Post*, August 26, 1986, https://www.washingtonpost.com/archive/politics/1986/08/26/drug-interdiction-effort-a-failure-governors-told/5c356a57-ebbf-400f-b37c-051c2b48fb55/.
[56] Ibid.
[57] Joel Brinkley, "4-Year Fight in Florida 'Just Can't Stop Drugs,'" *The New York Times,* September 4, 1986, https://www.nytimes.com/1986/09/04/us/4-yearfight-in-florida-just-can-t-stop-drugs.html.
[58] Bruce W. Jentleson, et al, *American Foreign Policy,5th ed.,* (New York: W.W. Norton, 2014), pp. 544

[59] Brown University, "Understanding the Iran-Contra Affair," *Brown* University, accessed on August 27, 2025, 2022, https://www.brown.edu/Research/Understanding_the_Iran_Contra_Affair/index.php.
[60] United States, Department of State, "The Reagan Doctrine, 1985," *U.S State Department*, accessed on August 27, 2025, https://2001-2009.state.gov/r/pa/ho/time/rd/17741.htm.
[61] United States of America Office of the Historian, "Central America, 1977-1980," accessed on August 27, 2025, https://history.state.gov/milestones/1977-1980/central-america-carter.
[62] United States Senate, "Drugs, Law Enforcement and Foreign Policy," p.36.
[63] Ibid, pp. 39-41.
[64] Ibid, p. 79.
[65] Mark Tran, "Manuel Noriega – From US Friend to Foe," *The Guardian*, April 27, 2010, https://www.theguardian.com/world/2010/apr/27/manuel-noriega-us-friend-foe.
[66] United States Senate, "Drugs, Law Enforcement and Foreign Policy," p. 82.
[67] Ibid, p. 83.
[68] Ibid, p. 85.
[69] Ibid, p. 93.
[70] Ibid, p. 97.
[71] Jonathan E. Sanford, "Honduras: U.S. Foreign Assistance Facts," March 31, 1987, *United States Congressional Research Service,* https://digital.library.unt.edu/ark:/67531/metacrs8841/m1/1/high_res_d/IB85080_1987Mar31.pdf.
[72] United States Senate, "Drugs, Law Enforcement and Foreign Policy," p.73.
[73] Ibid, pp.73-74.
[74] Ibid, p.79.
[75] Ibid, p.78.
[76] United States Department of State, "International Narcotics Control Strategy Report," March 1988, https://2009-2017.state.gov/documents/organization/102588.pdf, p.157.
[77] Julia Preston, "Cuba Details Drug Deals," *The Washington Post,* June 23, 1989, https://www.washingtonpost.com/archive/politics/1989/06/23/cuba-details-drug-deals/d54053bc-7a1f-476b-8080-ba9ee72bbb9d/.
[78] United States Congressional Research Service, "Cuba-U.S. Relations: Chronology of Key Events 1959-1999," *U.S. Congressional Research* Service, December 14, 1999 https://crsreports.congress.gov/product/pdf/RL/RL30386
[79] United States Senate, "Drugs, Law Enforcement and Foreign Policy," pp.15-16.
[80] Ibid, p.22.
[81] Ibid.
[82] Daniel Southerland, "Reagan's Foreign Policy Goes on Trial in Caribbean," *Christian Science Monitor*, August 29, 1984, https://www.csmonitor.com/1984/0829/082916.html.
[83] Vanda Felbab-Brown, "Counternarcotics Policy Overview: Global Trends & Strategies," *Brookings,* October 2008, https://www.brookings.edu/wp-content/uploads/2016/07/counternarcotics_policy_felbabbrown.pdf, p.15.
[84] Tristan Bove, "Drug Use is on the Rise as U.S. Spending on the War on Drugs Tops $1 Trillion and Cartel Leaders Drive Violent Eruptions in Mexico," *Fortune*, February 23, 2026, https://fortune.com/2026/02/23/us-trillion-dollar-drug-war-rising-use/.
[85] Sarah Shamin, "Is Venezuela the Big Cocaine Mance Trump Claims it to be?," *Al Jazeera*, September 4, 2025, https://www.aljazeera.com/news/2025/9/4/is-venezuela-the-big-cocaine-menace-trump-claims-it-to-be.
[86] Sean Mowbray, "All Coked Up: The Global Environmental Impacts of Cocaine," *Mongabay,* April 4, 2022, https://news.mongabay.com/2022/04/all-coked-up-the-global-environmental-impacts-of-cocaine/.
[87] Conor Lennon, "'Vicious Cycle' of Supply and Demand Fueling Cocaine Use," *United Nations News,* June 26, 2024, https://news.un.org/en/interview/2024/06/1151426.
[88] Muggah, "The Geopolitics of Trump's War on Drugs."
[89] Ibid.
[90] Zita Ballinger Fletcher, "Drug Trafficking as Irregular Warfare — And What Can be Done About It," *Military Times*, March 27, 2025, https://www.militarytimes.com/opinion/2025/03/28/drug-trafficking-as-irregular-warfare-and-what-can-be-done-about-it/.
[91] Giuseppe De Magistris, "A Proposal for a NATO High-Readiness Constabulary Force," *Center of Excellence for Stability Police Units Magazine, Number 2*, 2023, https://anyflip.com/wnmbd/zdec, p.44.
[92] Hugo Balta, "The Return of American Imperialism," *The Fulcrum*, September 6, 2025, https://thefulcrum.us/ethics-leadership/trump-caribbean-airstrike-tren-de-aragua-imperialism.
[93] Ibid.
[94] Amir Daftari et al, "Map Show Where US B-52 Bombers Deployed on Venzuela's Doorstep," *Newsweek,* October 15, 2025, https://www.newsweek.com/map-shows-where-us-b-52-bombers-deployed-on-venezuelas-doorstep-10884179.

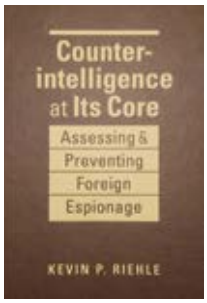
[95] Amir Daftari, "Trump Tightens Noose Around Venezuela," *Newsweek,* October 8, 2025, https://www.newsweek.com/trump-tightens-noose-around-venezuela-10846184; Allen Frazier, "What U.S. Forces Face as Venezuela Puts Russian-Armed Military on Wartime Alert," *Military.com*, October 20, 2025, https://www.military.com/daily-news/investigations-and-features/2025/10/20/what-us-forces-face-venezuela-puts-russian-armed-military-wartime-alert.html.

[96] Ron MacCammon, "Venezuela's Gray War: A Criminal Army, a Migrant Wave, and the U.S. 'Invasion,'" *Small Wars Journal*, May 28, 2025,https://smallwarsjournal.com/2025/05/28/venezuelas-gray-war-a-criminal-army-a-migrant-wave-and-the-us-invasion/.

[97] Sylvia Longmire, et al, "Redefining Terrorism: Why Mexican Drug Trafficking is More than Just Organized Crime," *Journal of Strategic Security*, volume 1, number 1, November 2008, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1044&context=jss.

Counterintelligence at Its Core: Assessing & Preventing Foreign Espionage

By Kevin P. Riehle
ISBN: 978-1962551489

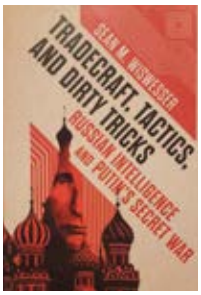


The Russian FSB: A Concise History of the Federal Security Service

By Kevin P. Riehle
ISBN: 978-1647124106

Tradecraft, Tactics, and Dirty Tricks: Russian Intelligence and Putin's Secret War

By Sean M. Wiswesser
ISBN: 978-1682476017



Reviewed by. Michael W. Parrott
Adjunct Professor, National Intelligence University

Michael W. Parrott is a veteran U.S. Army Counterintelligence (CI) Technician and an adjunct professor at the National Intelligence University (NIU), where he teaches graduate level seminars on special operations, CI, insider threat, and strategic intelligence competition. He specializes in gray zone & irregular warfare, CI mindset reform, and the integration of academic rigor with operational relevance for senior government and Intelligence Community audiences.

Introduction

This extended review essay examines three complementary works that illuminate the strategic, analytic, and operational dimensions of contemporary intelligence competition while assessing their value for scholars and practitioners. Dr. Kevin Riehle's *The Russian FSB: A Concise History of the Federal Security Service* (2024) traces the institutional lineage and governing logic of Russia's domestic security apparatus from its Tsarist and Soviet predecessors to the present. His *Counterintelligence at Its Core: Assessing and Preventing Foreign Espionage* (2025) offers a rigorous analytic framework for counterintelligence (CI) practitioners seeking decision advantage in strategic competition. These academic perspectives are complemented by Sean W. Wiswesser's *Tradecraft, Tactics, and Dirty Tricks: Russian Intelligence and Putin's Secret War* (2026), which draws on nearly three decades of CIA operational experience to illustrate how Russian intelligence tradecraft functions in practice. Considered together, these works form a strategic–analytic–operational triad that is highly relevant to irregular warfare (IW) and contemporary intelligence competition. They show how intelligence services function not merely as collectors of information, but as political instruments that shape competition below the threshold of armed conflict. As strategic competition increasingly unfolds through persistent engagement and grayzone campaigns, intelligence and CI have become central mechanisms of IW rather than support functions. Understanding this environment requires integrating how intelligence services are structured, how they generate decision advantage, and how tradecraft operates in practice—the synthesis this review seeks to provide. For practitioners and scholars of IW, these works demonstrate that intelligence competition is not ancillary to gray-zone conflict but constitutive of it—shaping political outcomes through persistent, adaptive engagement rather than episodic crisis response.

Intelligence Competition and the Irregular Battlespace

Contemporary IW cannot be fully understood apart from intelligence competition, because espionage, CI, covert influence, and political subversion increasingly shape strategic outcomes below the threshold of armed conflict. Rather than unfolding primarily through overt military confrontation, modern strategic competition increasingly manifests through espionage, CI, covert influence, and political subversion. These activities operate persistently below the threshold of armed conflict, shaping the strategic environment long before—and often instead of—kinetic engagement.

Understanding this environment requires more than episodic attention to intelligence scandals or isolated tradecraft narratives; it requires a comparative analysis of institutional structure, analytic method, and operational practice. Intelligence, IW practitioners and scholars require an integrated appreciation of how intelligence services are structured, how they analyze adversaries and threats, and how they operate in practice. Three recent works collectively address these dimensions. Kevin Riehle's *The Russian FSB* offers an institutional and historical foundation for understanding Russia's security services as instruments of political power. His *Counterintelligence at Its Core* provides analytic rigor to a field often constrained by definitional ambiguity. Sean Wiswesser's *Tradecraft, Tactics, and Dirty Tricks* supplies the operational perspective, grounding analytic and institutional insights into lived experience.

This essay evaluates the three works as a comparative body of knowledge, assessing their empirical rigor, analytic utility, and relevance to contemporary intelligence competition for both practitioners and scholars. Read together, the works form a strategic,

analytic, and operational triad that clarifies how Russian intelligence services shape competition below the threshold of war, while also revealing the limits of each author's evidentiary approach.

The Russian FSB and the Architecture of State Power

Riehle's *The Russian FSB: A Concise History of the Federal Security Service* is one of the clearest and most empirically grounded English-language studies of Russia's primary internal security organization. By tracing a lineage from the Tsarist *Okhrana* through the Soviet *Cheka* and KGB to the contemporary FSB, Riehle shows that continuity, rather than rupture, defines Russian state security practice.[1]

A core contribution of the book is its treatment of the FSB as a political instrument, not merely a security or law-enforcement body. Drawing extensively on Russianlanguage primary sources, Riehle shows how *chekist* identity, institutional mythology, and historical continuity shape modern Russian conceptions of internal security. His delineation of the FSB's six principal mission areas—CI, counterterrorism, crime suppression, intelligence, border security, and information security—reveals a scope far broader than that of most Western domestic security services.[2] Riehle shows how the FSB's institutional DNA turns deception, coercion, and political control into governing logics. This aligns with recent scholarship describing Russia as a 'hybrid intelligence state,' although the concept is most useful when treated as an analytical framework rather than a total explanation of Russian governance.[3] Thus, embedding *chekist* mythology into Russian national identity and glorifying the department's intelligence exploits for future generations.[4]

The book's limitations are primarily analytical rather than substantive. Internal bureaucratic politics, digital authoritarianism, and post-2022 Ukraine invasion institutional failures receive less sustained analysis than they deserve.[5] Nevertheless, *The Russian FSB* succeeds in its central purpose: showing that Russian intelligence services function as mechanisms of regime preservation.[6] For IW practitioners, this insight is foundational, particularly when assessing Russia's use of intelligenceled hybrid and grayzone strategies.

Counterintelligence Analysis and Decision Advantage

If *The Russian FSB* explains institutional form, *Counterintelligence at Its Core* explains analytic function. In this volume, Riehle confronts persistent ambiguity surrounding CI by defining CI as activity, threat mitigation, and analysis.[7] From this foundation, he advances a clear proposition: CI analysis exists to generate decision advantage in competitive environments defined by deception, uncertainty, and adversarial adaptation.[8]

Riehle's fourpart analytic taxonomy—foreign intelligence threat analysis, counterCI analysis, support to CI activities, and strategic CI analysis—provides conceptual clarity to a discipline often reduced to reactive investigations.[9] This taxonomy is one of the book's most valuable contributions because it offers a structured approach that aligns with and extends contemporary analytic literature, including Heuer's *Psychology of Intelligence Analysis* and Marrin's work on analytic professionalism.[10] He defines CI across three domains—activity, threat mitigation, and analysis—building on U.S. doctrine such as Executive Order 12333 and translating it into a more usable analytic framework.[11] The framework is particularly useful for professional education because it gives CI practice a structured logic linked to strategic outcomes.

Historical case studies, including the defection of Igor Gouzenko in 1945, illustrate how CI analysis can reveal adversary priorities, methods, and intent.[12] Although the book relies primarily on Western cases and addresses cyber-enabled and private-sector threats only indirectly, its analytic

rigor and clarity still make it a valuable contribution. For IW practitioners, Riehle's focus on decision advantage underscores the importance of intelligence analysis in shaping adversary perceptions, decisions, and behavior.

Tradecraft and Operational Reality

Sean Wiswesser's *Tradecraft, Tactics, and Dirty Tricks* provides the operational dimension that complements Riehle's academic analyses. Drawing on 28 years of service as a CIA operations officer, Wiswesser argues that Russian intelligence services sustain a continuous secret war against the United States and its allies, viewing them as the *glavniy protivnik*, or main enemy.[13]

Wiswesser's strength lies in his practitioner-oriented exposition of tradecraft. His discussion of recruitment, deception, surveillance detection, and non-official cover operations illustrates how institutional culture translates into operational behavior, though the narrative form limits generalization.[14] He highlights recurring features of Russian intelligence practice, including sexual *kompromat* (sex-espionage), cultivation of sympathetic intermediaries, fabricated reporting, and internal corruption.[15] These examples align with historical analyses of Soviet and Russian active measures, including Thomas Rid's *Active Measures* and Christopher Andrew's work on the KGB, which help place Wiswesser's observations in a longer analytic tradition.[16, 17]

The limitations of the work stem from its narrative genre and its dependence on anecdotal experience. Anecdotal evidence resists systematic generalization, and broader institutional and political constraints receive limited treatment. Yet this operational realism is also what gives the book much of its value. When read alongside Riehle's institutional and analytic frameworks, Wiswesser's account provides useful operational context, showing how doctrine and culture manifest in real-world intelligence operations.

A Strategic–Analytic–Operational Synthesis

Taken together, these three works form a coherent triad for understanding modern intelligence competition, as shown in Table 1.

The Russian FSB addresses the strategic and institutional foundations of Russian intelligence power. *Counterintelligence at Its Core* provides the analytic and methodological tools needed to understand and counter modern intelligence threats. *Tradecraft, Tactics, and Dirty Tricks* offer the operational and tactical perspective that connects theory to practice. While grounded in the Russian case, the analytic and CI frameworks may also have broader applicability to other authoritarian or intelligence-centric regimes, such as China or Iran, though such transfer requires caution.

Despite their methodological differences, the works converge on several themes central to IW: intelligence as a political instrument, deception and counter-deception as governing logic, the fusion of intelligence and governance in authoritarian systems, and the importance of decision advantage in strategic competition, as summarized in Table 2. Their differences are complementary and, taken together, yield a more complete understanding than any single perspective could provide.

Conclusion

For readers of *PRISM* and the Irregular Warfare Center (IWC), these works merit attention not simply as a unified body of study, but as complementary contributions that address distinct levels of intelligence competition. Riehle's institutional and analytic contributions establish the structural and cognitive foundations for understanding intelligence competition. Wiswesser's practitioner

account grounds those foundations in operational reality and shows how tradecraft functions in practice. Together, the books show that intelligence is not a supporting function in contemporary IW; it is among the principal mechanisms, and CI should therefore be treated as a core instrument of strategic competition. In an era shaped by hybrid threats, influence operations, and persistent espionage, effective scholarship and practice require the combined study of history, analysis, and tradecraft.

Table 1. Comparative Overview of Reviewed Works

Dimension	*The Russian FSB* (Riehle, 2024)	*Counterintelligence at Its Core* (Riehle, 2025)	*Tradecraft, Tactics, and Dirty Tricks* (Wiswesser, 2024)
Focus	Institutional history and structure of FSB	CI analytic methodology and taxonomy	Russian operational tradecraft and field tactics
Level of Analysis	Strategic-institutional	Analytic-methodological	Operational-tactical
Primary Sources	Russian-language archival and open sources	Western CI cases, historical defection cases	Firsthand CIA operational experience
Key Contribution	Maps FSB institutional DNA from Okhrana to present	Four-part CI analysis taxonomy for decision advantage	Practitioner lens on Russian intelligence culture
Limitations	Limited digital-era and post-2022 analysis	Western-centric case selection; limited cyber integration	Anecdotal; limited institutional/political context
IW Relevance	Shows intelligence as political instrument in hybrid warfare	Provides analytic framework for adversary assessment	Demonstrates how tradecraft shapes irregular battlespace

Source: Author.

Table 2. Methodological Comparison Matrix

Methodological Dimension	Riehle — *The Russian FSB*	Riehle — *CI at Its Core*	Wiswesser — *Tradecraft*
Research Approach	Archival / area-studies	Taxonomic / typological	Experiential / narrative
Source Base	Russian-language primary documents	Western IC frameworks and historical cases	Firsthand operational experience
Analytic Mode	Institutional-structural	Classificatory-analytic	Descriptive-anecdotal
Epistemological Orientation	Empiricist-historical	Rationalist-systematic	Pragmatist-practitioner
Generalizability	High for Russian security services	Moderate; Western-centric framework	Low; case- and context-dependent
Complementary Value	Provides institutional depth and historical continuity	Provides analytic clarity and decision framework	Provides operational authenticity and tactical realism

Source: Author.

Endnotes

[1] Kevin P. Riehle, *The Russian FSB: A Concise History of the Federal Security Service* (Washington, DC: Georgetown University Press, 2024).

[2] Riehle, *The Russian FSB*, 69-99.

[3] Jardar Østbø, "The Russian Hybrid Intelligence State," Intelligence and National Security 39, no. 6 (2024).

[4] Kevin P. Riehle, *Russian Intelligence: A CaseBased Study of Russian Services and Missions Past and Present* (Bethesda, MD: National Intelligence Press, 2022).

[5] Brian Taylor, *The Code of Putinism* (New York: Oxford University Press, 2018).

[6] Andrei Soldatov and Irina Borogan, *The Red Web* (New York: PublicAffairs, 2015).

[7] Kevin P. Riehle, *Counterintelligence at Its Core: Assessing and Preventing Foreign Espionage* (Boulder, CO: Lynne Rienner Publishers, 2025).

[8] Riehle, *Counterintelligence at Its Core*, 8-9.

[9] Riehle, 29-35.

[10] Exec. Order No. 12333, *United States Intelligence Activities* (1981).

[11] Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington, DC: CIA Center for the Study of Intelligence, 1999); Stephen Marrin, "Improving Intelligence Analysis," *International Journal of Intelligence and Counterintelligence* 24, no. 4 (2011).

[12] Riehle, *Counterintelligence at Its Core, 97-104.*

[13] Sean W. Wiswesser, *Tradecraft, Tactics, and Dirty Tricks: Russian Intelligence and Putin's Secret War* (Annapolis, MD: Naval Institute Press, 2024).

[14] Wiswesser, *Tradecraft, Tactics, and Dirty Tricks*, 40-126.

[15] Wiswesser, 112-145.

[16] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

[17] Christopher Andrew, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999).

Bibliography

Andrew, Christopher. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 1999.

Heuer, Richards J. *Psychology of Intelligence Analysis*. Washington, DC: CIA Center for the Study of Intelligence, 1999.

Hoffman, Frank G. "Hybrid Warfare and Challenges." *Joint Force Quarterly* 52 (1st Quarter 2009): 34–39.

Mazarr, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Carlisle, PA: U.S. Army War College Press, 2015.

Marrin, Stephen. "Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice." *International Journal of Intelligence and Counterintelligence* 24, no. 4 (2011): 697–719.

Østbø, Jardar. "The Russian Hybrid Intelligence State." *Intelligence and National Security* 39, no. 6 (2024).

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.

Riehle, Kevin P. *Counterintelligence at Its Core: Assessing and Preventing Foreign Espionage*. Boulder, CO: Lynne Rienner Publishers, 2025.

———. *The Russian FSB: A Concise History of the Federal Security Service*. Washington, DC:

Georgetown University Press, 2024.

———. *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present*. Bethesda, MD: National Intelligence Press, 2022.

Soldatov, Andrei, and Irina Borogan. *The Red Web*. New York: PublicAffairs, 2015.

Taylor, Brian. *The Code of Putinism*. New York: Oxford University Press, 2018.

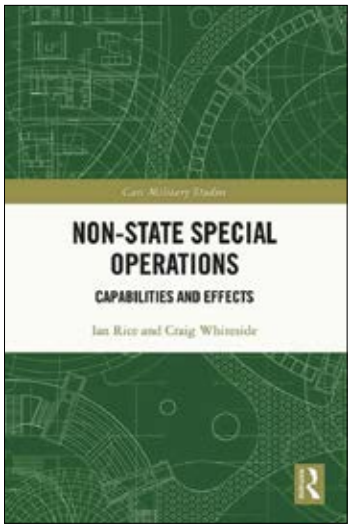
United States. Executive Order 12333. *United States Intelligence Activities*. 1981.

Wiswesser, Sean W. *Tradecraft, Tactics, and Dirty Tricks: Russian Intelligence and Putin's Secret War*. Annapolis, MD: Naval Institute Press, 2024.

Non-State Special Operations: Capabilities and Effects

By Ian Rice and Craig Whiteside
ISBN: 9781032594514

Reviewed by Dr. Kevin D. Stringer



With their refreshingly unique book on non-state special operations, Ian Rice and Craig Whiteside have significantly advanced the study of special operations by examining their use by several categories of violent non-state actors (VNSAs). Building upon their chapter in the edited volume *Into the Void: Special Operations Forces after the War on Terror*, the authors substantially expand upon their premise that non-state actors actively plan and conduct special operations to achieve strategic effects within a larger campaigning framework. In a highly structured, logical, and methodologically sound manner, the book carefully embeds VNSA special operations within the existing but incomplete theories of special operations, and then through a typology of four non-state groupings—militants, proxies, criminals and violent cults, and mercenaries—systematically examine the special operations conducted by each type. Leaning on Colin Gray's framework for why states conduct special operations, Rice and Whiteside demonstrate that non-state special operations also follow the same logic: seeking advantages from economy of force and expansion of choice.

For this reviewer, three main points made this book a very valuable read: the special operations forces (SOF) and special operations paradox, Western biases neglecting the study of non-state special operations, and the case studies presented. First, through its examination of non-state actors, the book further develops and refines the contentious distinction between SOF and special operations. As Professor Kalev Sepp of the U.S. Naval Postgraduate School notes in the foreword, many policy makers hold the "erroneous view that any action by a designated SOF unit made it, by definition, a 'special' operation" (p. xiv). Conversely, the authors of this book convincingly claim that a non-state actor that does not have a standing SOF can use "*ad hoc* or specifically tailored organizations to perform special operations aimed

Colonel Kevin D. Stringer, USA (Ret.), Ph.D. is a lecturer at the University of Northwestern Switzerland, an Associate Editor of PRISM: The Journal of Complex Operations, and adjunct faculty at the Baltic Defence College in Estonia. With 30 years of commissioned military service, he served as a foreign area officer and strategist in the U.S. Special Operations community. His research and publications focus on special operations (https://drkevinstringer.com/).

to achieve outsized results" (p. 23). Most insightful was their articulation of a SOF and special operations paradox where: "Some state and non-state SOF do not regularly execute special operations, and states and non-states without SOF can execute special operations" (p. 24). From their research, most non-state formations that were designated as SOF were actually just elite forces. The VNSA special operations used as case studies were primarily conducted by ad-hoc groupings concentrated on an objective that could generate strategic outcomes.

A second insight from the book is that there seems to exist a double-sided Western bias that has resulted in disregarding the study of non-state special operations. This bias derives from an overly state-centric view of the application of force that relegates the conduct of special operations only to nation-states, with SOF research primarily conducted on the Anglo-American-European experience. A second, and potentially more serious aspect, is a seemingly hubristic view toward non-state opponents and their capabilities. Rice and Whiteside opine that if policy-makers, intelligence professionals, and senior military leaders had understood that the Islamic State's large-scale raid into Haditha in 2012, or the Abu Ghraib prison break in 2013, were actually sophisticated special operations and not anomalies or "lucky breaks" against Iraqi government forces, then they might have better assessed the rising strength and threat of the adversary, and its logic for using these special operations within the emerging "Breaking the Walls" campaign to establish a caliphate (pp. 36-42, 161). A better comprehension of VNSA logic for using special operations in the future could enable more effective countermeasures.

Finally, the case studies selected to buttress the book's claims and emerging theory were highly interesting and varied. They range from the 1947 Acre prison breakout by *Irgun* and the Stern Gang to the *Executive Outcomes* operations in Angola and Sierra Leone in the 1990s. Regardless of whether the reader agrees that all the cases depicted are special operations, the authors evaluate them consistently against their credible framework of analysis. This reviewer was particularly intrigued, and disturbed, by the 2007 military raid and hostage snatch operation executed against the U.S.-Iraqi Karbala Provincial Joint Coordination Center by the Shiite Iraqi Asa'ib Ahl al-Haq (AAH) group. With clandestine reconnaissance, subterfuge, and extensive mission planning, it met all the hallmarks of a special operation conducted by an Iranian proxy (pp. 87-93).

As noted in the conclusion, this book is "exploratory and an exercise in non-state special operations theory-building" (p. 160). Hence it does have two areas for potential refinement. First, the claim that criminals and violent cults use special operations to achieve their strategic goals remains far-fetched for this reader. The justifying cases seem "stretched" to fit the paradigm. Second, the category of "mercenary" is pejorative and harkens back to the 1960s, and United Nations' hyperventilation over Katangan and Biafran use of soldiers-of-fortune to achieve their respective independence. This reviewer recommends a different and updated terminology since this VNSA type seems to be extinct in the modern international security environment. Overall, though, with impeccable sources, superb methodology, and highly credible authors--both combat veterans with requisite academic and practitioner experience--this book is an essential library addition for all national security policymakers, practitioners, and scholars seeking to understand the full gamut of special operations. It fits nicely on the special operations bookshelf next to the aforementioned *Into the Void: Special Operations Forces after the War on Terror,* James Kiras' *Special Operations Success,* and Mark Grdovic's *Those Who Face Death: The Untold Story of Special Forces and the Iraqi Kurdish Resistance.*

SUBSCRIPTIONS

To request a hard copy of *PRISM: The Journal of Emerging Threats | Complex Statecraft*, contact the PRISM editorial staff at PRISM@irregularwarfarecenter.org. Please include your preferred mailing address and desired number of copies in your message. Note that supplies of hard copy may be limited due to high demand.

PRISM
SCIRE QUOD SCIENDUM

IRREGULAR
WARFARE CENTER